The Akenti Access Control System:
Resource Access Control with Authorization and Attribute Certificates[1]

(An Application of Public-key Infrastructure and Digitally Signed Certificates)

William E. Johnston[2], Srilekha Mudumbai, Mary Thompson, Gary Hoo, and Keith Jackson
Information and Computing Sciences Division
Ernest Orlando Lawrence Berkeley National Laboratory
University of California

2. wejohnston@lbl.gov (510-486-5014), mudumbai@george.lbl.gov, mrt@george.lbl.gov - http://www-itg.lbl.gov

Security for Widely Distributed Systems

Motivation:

Our scientific environment involves

- multi-user instruments at national facilities
- widely distributed supercomputers and large-scale storage systems
- data sharing in restricted collaborations
- network-based multimedia collaboration channels

and <u>these facilities, collaborations, and stakeholders are diffuse - geographically distributed and multi-organizational</u>.

These circumstances require

- distributed management - because the principals and resources are dispersed organizationally
- distributed access control - because the resources and users are dispersed geographically

Akenti Access Control System

Outline

- **Use a Well Understood Approach as a Model**
- **Overall Goals**
- **Background and Framework**
- **General Approach**
- **Implementation and Deployment Strategy**
- **The General Security Model for Access Control**
- **Policy Model**
- **Operation of the Akenti Access Control System**
- **Authorization Certificates for Apache**
- **Authorization Certificates for GSS-API**
- **Authorization Certificates for CORBA**
- **Certificate Infrastructure**
- **User Interaction**
- **Identity Establishment**
- **Use-conditions**
- **Attributes**
- **CDS: A Simple Akenti Application**
- **Bandwidth Reservation**
- **Monitoring**

Use a Well Understood Approach as a Model

♦ **Stakeholders are identified by (usually) written policy**

♦ **Representations of authority ("use-conditions") are made by written, signed procedures, memoranda, etc.**

♦ **The required use-conditions are satisfied by a set of attributes: organizational membership, training, etc.**

♦ **Who and/or what can attest to users' satisfaction of the use-conditions is established by policy: e.g. a token issued by a personnel department, a certificate of training issued by an accredited school, etc.**

♦ **Credential checking is usually based on an operational authority that compiles a list of stakeholder use-conditions and then validates the users' attributes against this list**

Akenti Access Control System: Model

(1) Use-conditions are Imposed by Independent Stakeholders

Stakeholders provide and maintain and use-conditions

DOE-HQ

LBNL

ALS

UC

Group PI

ALS Medical Beamline *

access control gateway

STOP

Memo
exclude "bad" countries

Memo
include all LBNL staff and guests

Memo
must have X-ray safety training

Memo
must have approved protocol

Memo
must be group member
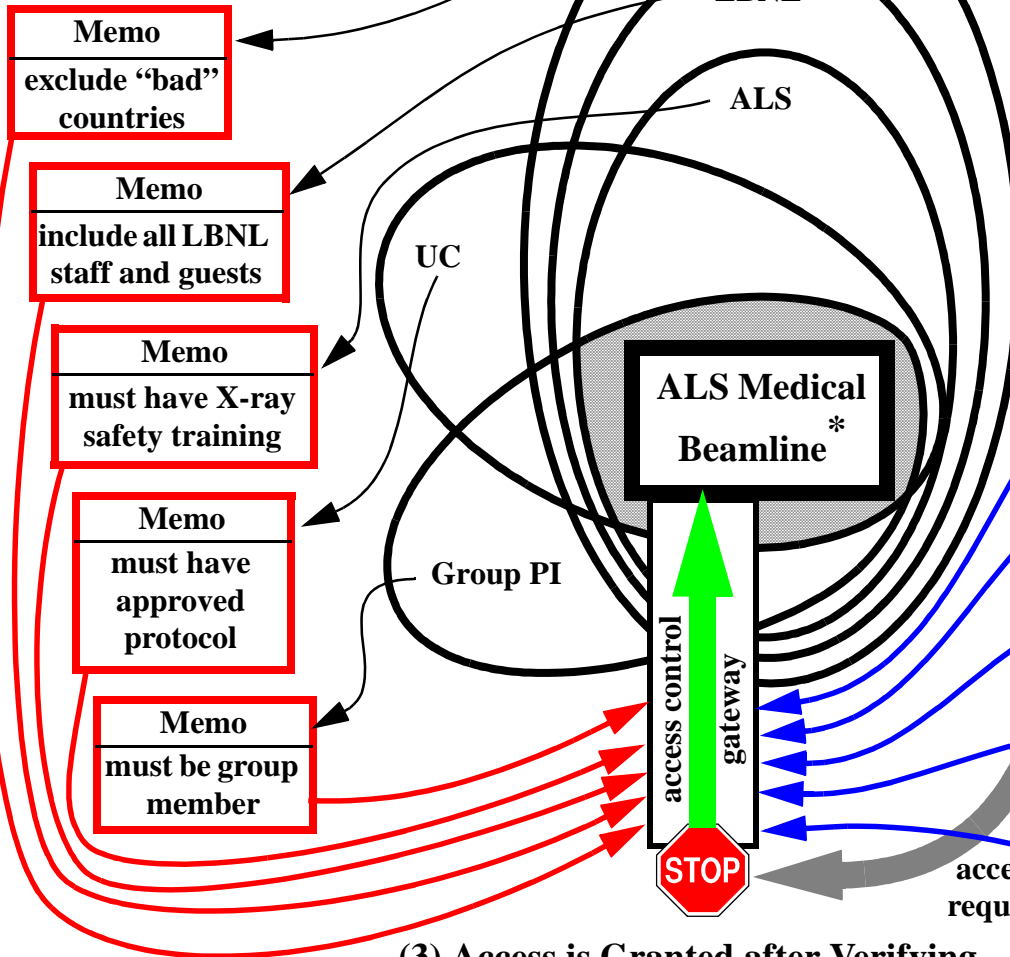
(2) Users have Attributes that Match the Use-conditions

Attribute certifiers that are trusted by the stakeholders

Passport agency → good country

LBNL Personnel Dept. → LBNL employee or guest

XYZ State University → X-ray 101

U.C. Human Use Committee → approved protocol

ALS Medical Beamline group PI → Medical R&D group

access request
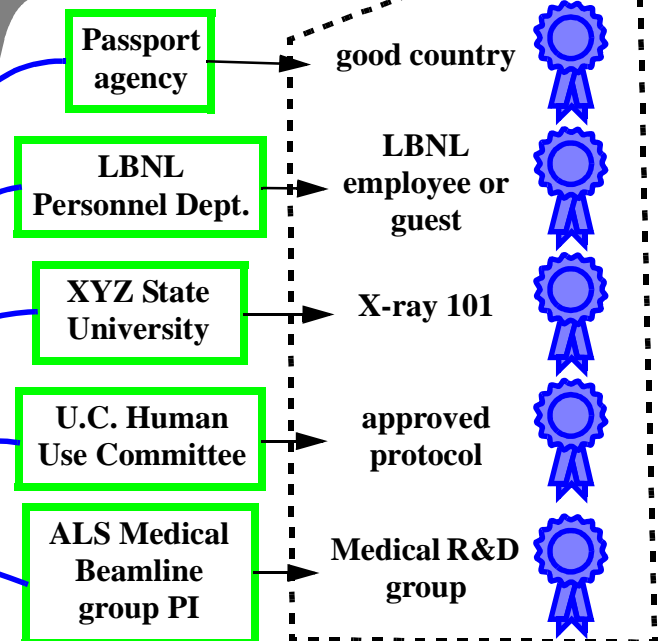
(3) Access is Granted after Verifying that User Attributes Match the Required Use-Conditions

* hypothetical

1   Societal Access Control Model

Akenti Access Control System: Model

♦ **All of the attributes that match use-conditions are likely to be packaged into a "capability" - a single document (e.g. a "license" or badge) that names the user, and perhaps the resource and the range of permitted actions**

♦ **The access control enforcer - a door guard, the experiment PI, etc. - typically just validates the capability (e.g., checks the license) when access is requested**

This general societal model provides us with the framework for an on-line architecture that accomplishes the same sort of access control for on-line resources.

Akenti Access Control System

Overall Goals

On-line access control for the scientific environment must provide:

♦ **Secure sharing of resources in a way the reflects currently accepted practice and principles:**
- **stakeholders independently make assertions about resource use**
- **trusted third-parties certify user attributes required for the use-conditions**
- **authenticated users that posses the required attributes easily gain access**
- **the level of credential checking (and security) is determined by the nature of the resource being protected**

◆ **Dynamic and easily used mechanisms for generation, maintenance, and distribution of the access control information**

  • those that make assertions (e.g. establish the use-conditions or attest to user attributes) must be able to do so within their own working environment (usability!)

◆ **Strong assurances that use-conditions are met**

  • access decisions must be made based on assured information and then enforced by strong security services

◆ **Provide a mechanism to separate access policies from identity policies**

  • akin to authorization certificates (e.g. X9.45)

Akenti Access Control System

Background and Framework

♦ **Digitally signed documents (an application of public-key cryptography) can provide**
  - **assured assertions (e.g. enumeration of resource use-conditions), and**
  - **user information (name and attributes)**
  without requiring the physical presence of the signer/certifier (in the same way that we accept holographically signed documents today).

♦ **Certification Authorities provide policy-based identity assurances in the form of widely distributed, digitally signed certificates that bind an identity to a public key (analogous, e.g., to a state issued driver's license) - one type of "signing authority"**

Akenti Access Control System: Background

♦ **Other signing authorities are the stakeholders that generate, sign, and distribute their assertions as certificates**

♦ **A policy engine and access control gateway identifies stakeholder imposed use-conditions and whether a potential user has met these use-conditions and makes access decision for, e.g., information systems, instruments, communications channels, computing and storage capacity**

♦ **Application-level security services that provide secure (confidential and reliable) end-to-end communication enforce access control decisions (e.g. SSL - the Secure Sockets Layer, and GSS - the IETF's General Security Services API)**

♦ **Web browsers (e.g. Netscape) and servers (e.g. Apache), and commercial Certification Authorities and directory servers, can provide a general infrastructure for managing certificates.**

Akenti Access Control System

General Approach

♦ **Use-condition / authorization certificates**: allow stakeholders to impose their requirements in a "natural and convenient" way - by representing them as digitally signed documents that are generated, maintained, and distributed in the stakeholder's "local" (working) environment.

♦ **Attribute certificates**: attribute certifiers ("verifiers") provide user characteristics that match use-conditions, again in a natural and convenient way.

♦ **Identity**: standard X.509 certificates and Certification Authority infrastructure are used for identifying and authenticating various entities.

Akenti Access Control System: Approach

◆ **<u>"Akenti" policy engine</u>: An independent software module that makes access decisions by**
  - **identifying all stakeholders' use-conditions associated with a resource,**
  - **searching for the corresponding user attributes, and**
  - **verifying that a potential user matches all stakeholder's use-conditions.**

◆ **<u>Capabilities</u>: For a given resource, Akenti provides a verified user identity, an assured access control decision, and a list of permitted actions. The application (or its agent) then uses these to control specific user actions and to set up a secure communication channel between the user/client and resource.**

Akenti Access Control System

Implementation and Deployment Strategy

♦ **Use as much existing and emerging technology as possible:**

  - **identity certificate generation and management is provided by Netscape Navigator (v4, and later), the Netscape, or comparable, CA and LDAP directory servers**

  - **security services are provided by SSL and GSS (for providing secure communication channels)**

♦ **The Akenti policy engine is being kept independent of the application and the security services.**

♦ **The Apache Web server is used as a prototype access control gateway for data and other services that can be invoked with cgi-bin scripts. The standard Apache access control module (*.htaccess*, etc.) is replaced by Akenti.**

Akenti Access Control System: Implementation

◆ **Java applications provide the mechanism for stakeholders and attribute certifiers to construct use-condition and attribute certificates.**

◆ **Any Web server "trusted" by the stakeholders and certifiers can be used to distribute the use-condition and attribute certificates.**

◆ **Akenti provides data driven certificate analysis: it does no semantic analysis of the use-conditions - that is left to the resource server, or to out-of-band agreements (i.e. as to what specific terms mean and their relationships to each other).**

Akenti Access Control System: Implementation

generate authoritative information

| **Certification Authorities (identity - e.g. X.509)** | **Attribute Authorities (user characteristics)** | **Authorization Authorities** (resource owner generated use-conditions) | digitally signed documents generated by many independent principals |

certificate servers
- ♦ identity
- ♦ use-conditions
- ♦ attributes

(trusted agents of the signing authorities)

authorize

certificate cache

policy engine
(acts on behalf of all stakeholders)
- ♦ ensure stakeholder representation
- ♦ evaluate policy and verify certificates (i.e., matches use-conditions and attributes)
- ♦ issue an access capability for an entity (user)

Stakeholder identities

auth req   resp

operate

user identity

authorization request

user client application
(e.g. Web browser)

access control gateway
- ♦ acquire capability from policy engine
- ♦ enforce "check immediate" requirements (e.g. re-authenticate user identity and/or use-condition certificates, collect payment, etc.)

security services
- ♦ set up security context between user-client and resource, using, e.g. Apache/SSL or SPKM/GSS

secure platform

resource
- ♦ fine-grained access control: enforce profiles of permitted actions, parameter ranges, time slots, etc.
- ♦ access content - e.g. data-objects, compute server, digital library, instruments, etc.

2   The Overall Architecture of the Authorization Certificate Approach

The General Security Model for Access Control

The security model is that the authorized "user community" (collection of identities that will be granted access) is defined by the intersection of a set of "use-condition" groups.

A Use-condition group is implicitly defined by a use-condition requiring an "attribute" (to be presented by a "user" in order to satisfy the use-condition).

Group are populated by designated "certifiers" who assign attributes to users.

So, the authorized community is the subset of identities that belong simultaneously to all of the use-condition groups for a resource environment.

Akenti Access Control System: Security Model

access-group
possessing the
attributes required by
all stakeholders

Stakeholder_1
requires Attribute_1
and Attribute_2

Stakeholder_2
requires Attribute_3
and Attribute_4

set of users
who posses
Attribute_3
and
Attribute_4

set of users who posses
Attribute_1 and
Attribute_2

sets of required
attributes define
access-groups

set of users
who posses
Attribute_5
and
Attribute_6

set of users
who posses
Attribute_6

Stakeholder_3
requires Attribute_5
and Attribute_6

separate attributes
may be required
for specific actions
on the resource

Stakeholder_4
requires Attribute_6
for Action_1

3   **Access Groups are Defined by Several Required Attributes**

Akenti Access Control System: Security Model

This security model is intended to support a variety of policy models, including flat and hierarchical authority, and decentralized and centralized management of access conditions.

The security model provides for controlling access to resources through restrictions imposed by several types of use-conditions that are defined independently by multiple stakeholders:

- access groups are defined implicitly by requiring a set of attributes
- actions on resources may be further restricted by requiring additional attributes (evaluated independently of access)
- operational requirements (e.g. time-of-day) are defined and satisfied by "data fields" in attribute certificates (and then acted on by the security gateway or resource server)

Akenti Access Control System

Policy Model

A *policy model* is built on a general security model in a way that will support the access/use policies required in a particular resource domain.

The characteristics of a particular policy model - e.g. hierarchical authority with delegation - is a function of the resource / application domain.

A hierarchical policy model is implemented using the Apache Web server: the specification of resource stakeholders (i.e. who can set use-conditions) is evaluated from the point of attempted access, up to the root of the Web server directory structure. This allows for multiple, independent, hierarchically related stakeholders (who can impose use-conditions at and below the directory that they control, but not above) and it allows for delegation of authority if

the Web service (e.g. ImgLib) provides for users creating directories and specifying who can set use conditions.

Akenti: Policy Model

LBNL Image Library -- Top-level Index

Digital Library ①
♦ **owned by Webmaster**
♦ **resources allocated by policy**
♦ **designates collection owners**

LBNL Image Library -- Top-level Index

Widget Project Collection
♦ **owned by project PI**
♦ **available only to project**

Lung Collaboration collection summary ②
♦ **owned by collaboration curator**
♦ **available to DOE Labs and collaborators**

4 Example Policy Model for a Digital Information Repository:
Hierarchical domains of control and access rights

LBNL Image Library -- Collection LUNG_STRUCTURE

Group summary data ③
♦ **owned by group curators**
♦ **available to collaboration only**

Individual investigator's data ④
♦ **owned by investigator**
♦ **available only to investigator and co-workers**

Akenti: Policy Model

http://ImgLib.lbl.gov

required_attribute **CN="Mary Thompson"**
*enables (***read** *and* **write** *and* **create_col***)*
for **http://ImgLib.gov/Lung_Collab**
with scope **sub-tree**
issuer= Webmaster
①

♦ The <u>Webmaster delegates</u> to Mary Thompson the authority to manage the *Lung_Collab* collection.

Lung_Collab

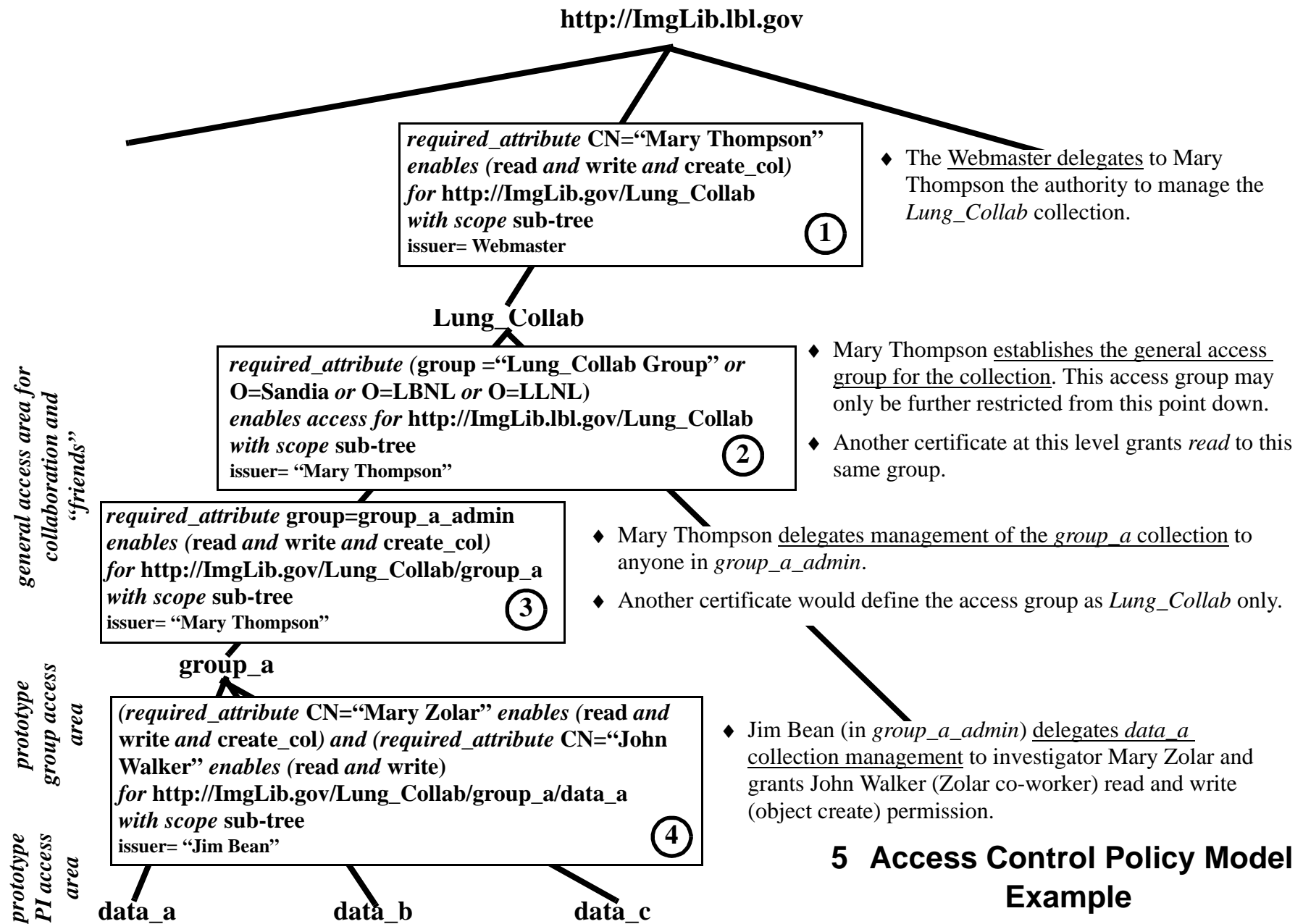*required_attribute (***group ="Lung_Collab Group"** *or*
O=Sandia *or* **O=LBNL** *or* **O=LLNL***)*
enables access for **http://ImgLib.lbl.gov/Lung_Collab**
with scope **sub-tree**
issuer= "Mary Thompson"
②

♦ Mary Thompson <u>establishes the general access group for the collection.</u> This access group may only be further restricted from this point down.

♦ Another certificate at this level grants *read* to this same group.

required_attribute **group=group_a_admin**
*enables (***read** *and* **write** *and* **create_col***)*
for **http://ImgLib.gov/Lung_Collab/group_a**
with scope **sub-tree**
issuer= "Mary Thompson"
③

♦ Mary Thompson <u>delegates management of the *group_a* collection</u> to anyone in *group_a_admin*.

♦ Another certificate would define the access group as *Lung_Collab* only.

group_a

(required_attribute **CN="Mary Zolar"** *enables (***read** *and*
write *and* **create_col***) and (required_attribute* **CN="John Walker"** *enables (***read** *and* **write***)*
for **http://ImgLib.gov/Lung_Collab/group_a/data_a**
with scope **sub-tree**
issuer= "Jim Bean"
④

♦ Jim Bean (in *group_a_admin*) <u>delegates *data_a* collection management</u> to investigator Mary Zolar and grants John Walker (Zolar co-worker) read and write (object create) permission.

5 Access Control Policy Model Example

data_a   **data_b**   **data_c**

general access area for collaboration and "friends"

prototype group access area

prototype PI access area

Imaging and Distributed Computing Group,
Information and Computing Sciences Division

Akenti Access Control System
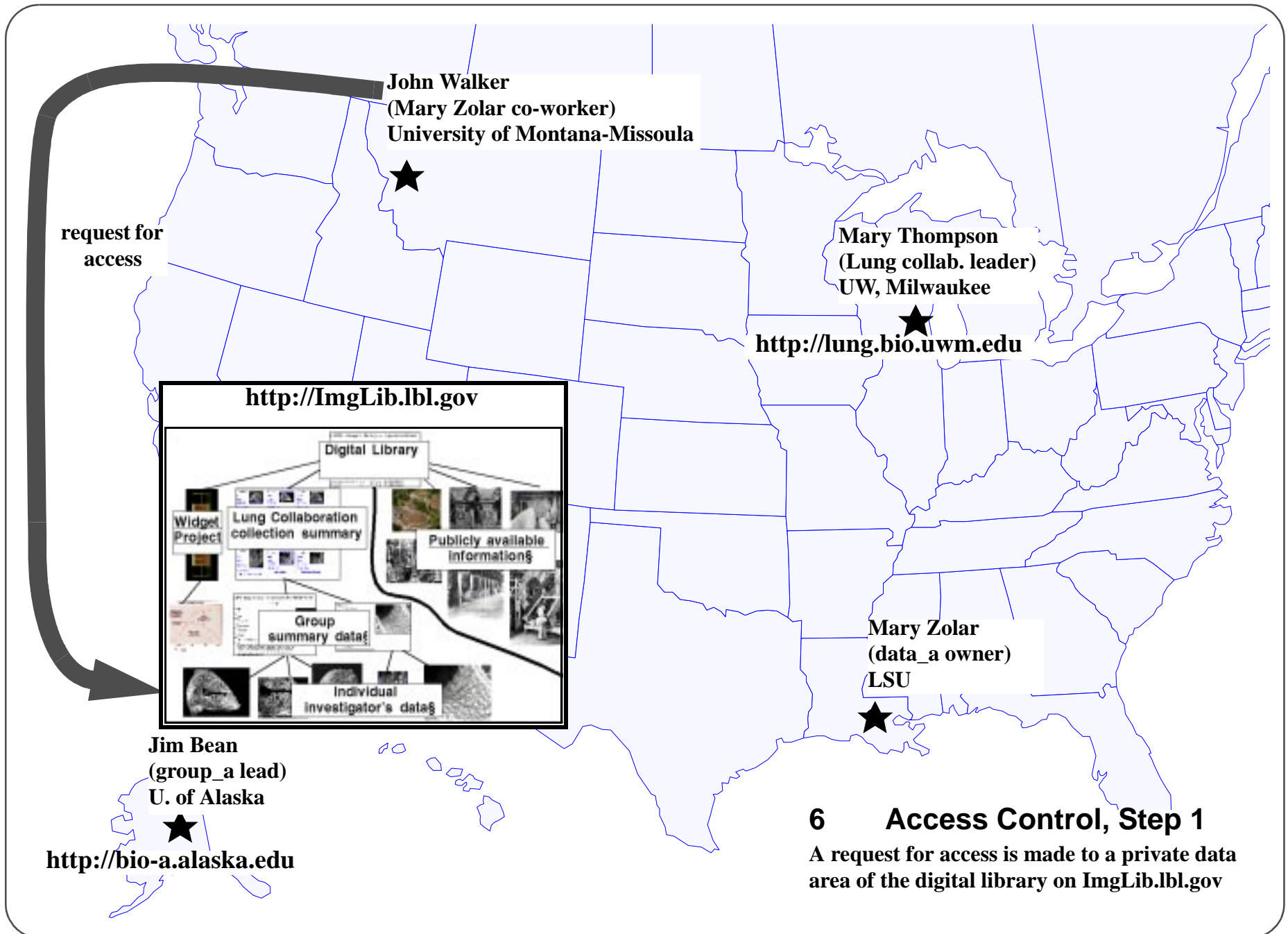
Operation of the Akenti Access Control System

Akenti is an implementation of the "policy engine" component in the architecture illustrated in figure 2. It provides:

- **an interface for acquiring a specification of the general policy items (e.g. the resource name, who are the stakeholders, which are the trusted CAs, etc.)**
- **acquisition and verification of all related certificates**
- **matching of (uninterpreted) use-conditions and attributes**
- **implementation of a policy model (e.g. what are the relationships among the stakeholders)**
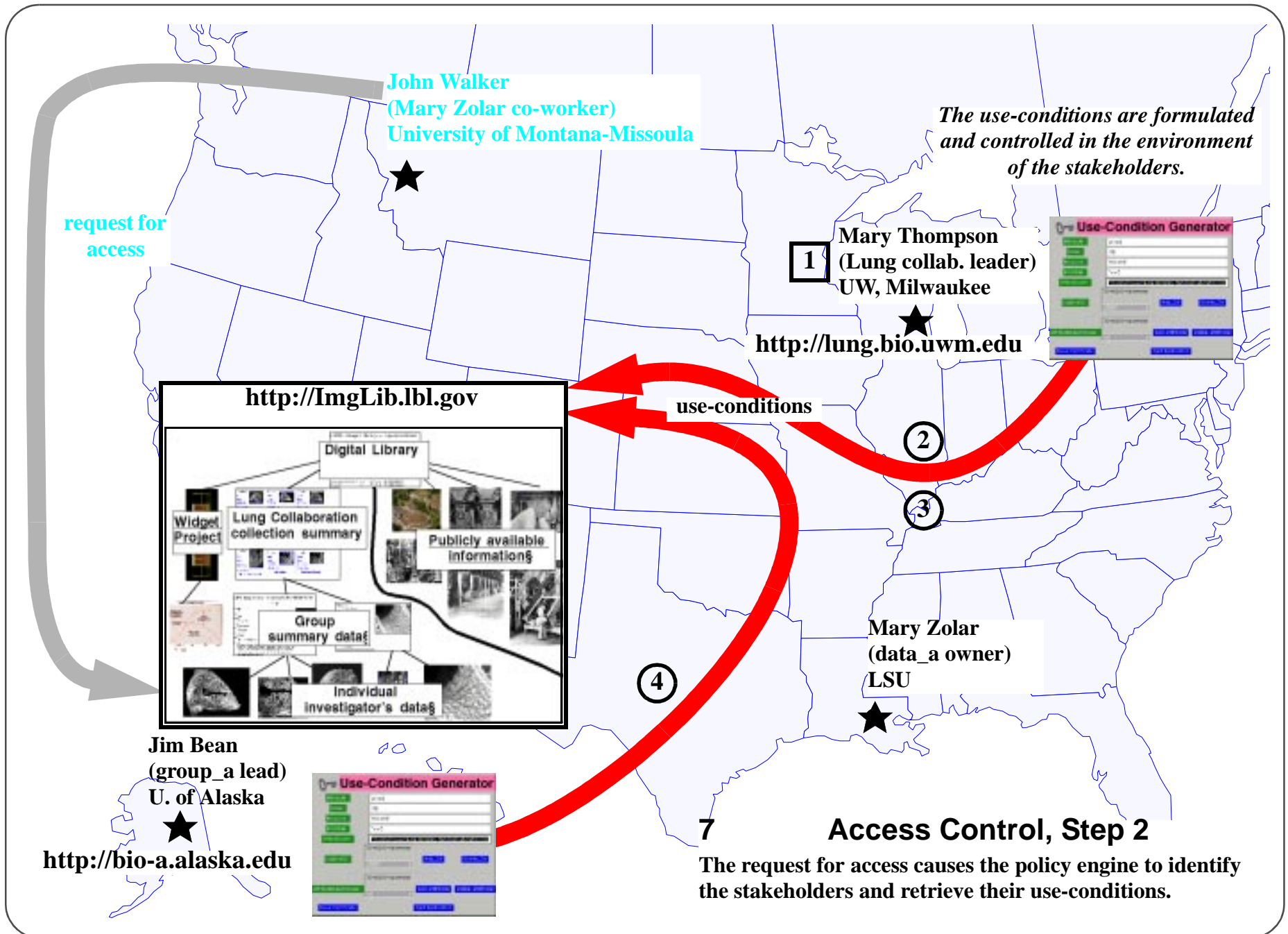- **passing the resulting "capability" to the resource controller**

The following figures illustrate the flow of control and information in the Akenti access control system relative to the policy model illustrated in figures 4 and 5, above.
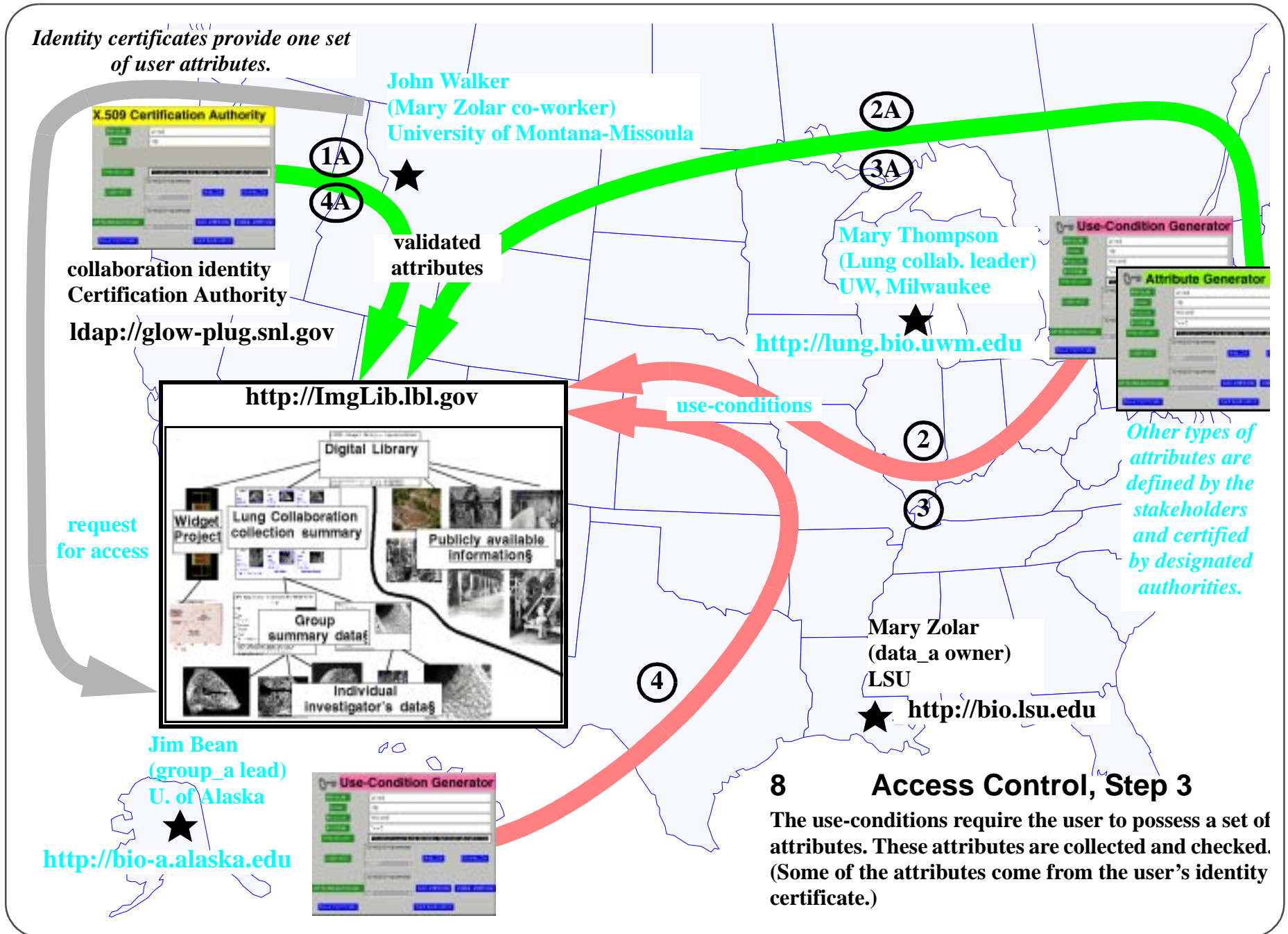
Akenti Access Control System: Operation

John Walker
(Mary Zolar co-worker)
University of Montana-Missoula

★

request for access

Mary Thompson
(Lung collab. leader)
UW, Milwaukee

★

http://lung.bio.uwm.edu

http://ImgLib.lbl.gov

Digital Library

Widget Project

Lung Collaboration collection summary

Publicly available information§

Group summary data§

Individual investigator's data§

Mary Zolar
(data_a owner)
LSU

★

Jim Bean
(group_a lead)
U. of Alaska

★

http://bio-a.alaska.edu

6   Access Control, Step 1

A request for access is made to a private data area of the digital library on ImgLib.lbl.gov

Akenti Access Control System: Operation

John Walker
(Mary Zolar co-worker)
University of Montana-Missoula

The use-conditions are formulated and controlled in the environment of the stakeholders.

request for access

1 Mary Thompson
(Lung collab. leader)
UW, Milwaukee

http://lung.bio.uwm.edu

Use-Condition Generator

http://ImgLib.lbl.gov

Digital Library

Widget Project

Lung Collaboration collection summary

Publicly available information§

Group summary data§

Individual investigator's data§

use-conditions

2

3

4

Mary Zolar
(data_a owner)
LSU

Jim Bean
(group_a lead)
U. of Alaska

Use-Condition Generator

http://bio-a.alaska.edu

7 **Access Control, Step 2**

The request for access causes the policy engine to identify the stakeholders and retrieve their use-conditions.

Akenti Access Control System: Operation

Identity certificates provide one set of user attributes.

X.509 Certification Authority

**John Walker
(Mary Zolar co-worker)
University of Montana-Missoula**

2A

1A

3A

4A

validated attributes

collaboration identity Certification Authority

ldap://glow-plug.snl.gov

**Mary Thompson
(Lung collab. leader)
UW, Milwaukee**

Use-Condition Generator

Attribute Generator

http://lung.bio.uwm.edu

http://ImgLib.lbl.gov

Digital Library

Widget Project

Lung Collaboration collection summary

Publicly available information§

Group summary data§

Individual investigator's data§

use-conditions

2

3

Other types of attributes are defined by the stakeholders and certified by designated authorities.

request for access

**Mary Zolar
(data_a owner)
LSU**

4

http://bio.lsu.edu

**Jim Bean
(group_a lead)
U. of Alaska**

Use-Condition Generator

http://bio-a.alaska.edu

8   Access Control, Step 3

The use-conditions require the user to possess a set of attributes. These attributes are collected and checked. (Some of the attributes come from the user's identity certificate.)

Akenti Access Control System: Operation

X.509 Certification Authority

John Walker
(Mary Zolar co-worker)
University of Montana-Missoula

(2A)

(1A)

(4A)

collaboration identity
Certification Authority

ldap://glow-plug.snl.gov

validated
attributes

secure
channel

(3A)

1

Mary Thompson
(Lung collab. leader)
UW, Milwaukee

http://lung.bio.uwm.edu

Use-Condition Generator

Attribute Generator

http://ImgLib.lbl.gov

Digital Library

Widget
Project

Lung Collaboration
collection summary

Publicly available
information§

Group
summary data§

Individual
investigator's data§

use-conditions

(2)

(3)

request
for access

Mary Zolar
(data_a owner)
LSU

http://bio.lsu.edu

(4)

Jim Bean
(group_a lead)
U. of Alaska

http://bio-a.alaska.edu

Use-Condition Generator

9   Access Control, Step 4

The access control decision (affirmative) is passed to th
Web server that then establishes a secure
communication channel to the requester.

Akenti Access Control System

Authorization Certificates for Apache

Akenti integrates with the unmodified Apache Web server by replacing the standard access control module ("htaccess").

Secure connection requests (https) pass the user identity certificate and the name of the requested resource to Akenti. Akenti then identifies all use-conditions, obtains the attribute certificates for the user, validates all certificates, and matches all use-conditions with attributes.

Akenti Application: Apache

generate authoritative information

Authorization Authorities (resource owner generated use-conditions)

Attribute Authorities (user characteristics)

Certification Authorities (identity - e.g. X.509)

certificate servers
- ♦ identity
- ♦ use-conditions
- ♦ attributes

(trusted agents of the signing authorities)

authorize

certificate cache manager
- ♦ cache all active certificates accounting for the cache time limits imposed by the stakeholders
- ♦ cache resource capabilities

policy engine
- ♦ identifies stakeholders
- ♦ acquires use-conditions
- ♦ identifies required attributes and issuers
- ♦ acquires attribute certificates
- ♦ validates certificates and matches use-conditions and attributes

stakeholder identities
- ♦ *.htauthority* files in resource directories
- ♦ stakeholder DN
- ♦ stakeholder CA
- ♦ stakeholder directory server
- ♦ permitted user CAs

secure platform

operate

user identity

auth. request

response ("denied" or a "capability")

authorization request

user client application (e.g. Web browser)

Apache
- ♦ pass user identity and resource name to Akenti
- ♦ acquire capability from policy engine

secure channel (SSL)
- ♦ set up security context between user-client and resource

resource
- ♦ fine-grained access control may be implemented by Web server resident methods that check for permitted actions
- ♦ finally the resource - data-object or cgi-bin program - is accessed

10   **Akenti Integrated with the Apache Web Server**

Akenti Application: Apache

Identify the stakeholders (*.htauthority*)

Establish explicit trust of CAs:

UserIdCertificateAuthority

"/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA"

"-----BEGIN CERTIFICATE-----\

MIICdDCCAd2gAwIBAgIBATANBgkqhkiG9w0BAQQFADBeMQswCQYDVQ\

QGEwJVUzEuMCwGA1UEChMlTGF3cmVuY2UgQmVya2VsZXkgTmF0aW9uYWwgTGFib3JhdG9yeTE\

NMA\

sGA1UECxMESUNTRDEQMA4GA1UEAxMHSURDRy1DQTAeFw05NzA4MjkxNjMwNDJaFw05OTA4M\

jkxNj\

MwNDJaMF4xCzAJBgNVBAYTAlVTMS4wLAYDVQQKEyVMYXdyZW5jZSBCZXJrZWxleSBOYXRpb2\

5hbC\

BMYWJvcmF0b3J5MQ0wCwYDVQQLEwRJQ1NEMRAwDgYDVQQDEwdJRENHLUNBMIGfMA0GCS\

qGSIb3DQ\

EBAQUAA4GNADCBiQKBgQDArly+tnX5eW7v4KT5CVf/IwR8rDkqniDUq34x/wqrKbM0AY+SV2hEHz\

+MCDgSlmPOXfwEplXW5IYYXqJ3+dK06et7mUodOhAB+0b6a8dVwul1+gRwEi80vft4+WvDUUHMZQ\

iq3UqFTsPN+09sW+2paqXNQZvBq2r+6/ovM4OqVwIDAQABo0IwQDAdBgNVHQ4EFgQUCQcdq1LvwV\

prM7kLlPLl7fmW4PswHwYDVR0jBBgwFoAUCQcdq1LvwVprM7kLlPLl7fmW4PswDQYJKoZIhvcNAQ\

EEBQADgYEAtcWt79TvzTl+zlkXBm8lqJPLXfsmwn0eaUGZiBkxhm5FGMUs02sUjaAUKiC6seR9xN\

E2C6EEJ7OyZRP7aqtNbbqeZBnUtCJN/iyFk9vQMMtJtTPr6uBbExhUaGFuJLMhHfMG/1pfDTIHQZ\

10Q0sF1ZmLyAdhiQBXekI5c5iheP4=\

-----ENDCERTIFICATE-----"

UserIdCertificateAuthority

"/C=US/O=Diesel Collaboratory/OU=SNL-CA/CN=glow-plug.ca.sandia.gov"

"-----BEGIN CERTIFICATE-----\

Akenti Application: Apache

MIICdjCCAd+gAwIBAgIBATANBgkqhkiG9w0BAQQFADBfMQswCQYDVQ\
QGEwJVUzEdMBsGA1UEChMURGllc2VsIENvbGxhYm9yYXRvcnkxDzANBgNVBAsTBlNOTC1DQTEg
MB\
4GA1UEAxMXZ2xvdy1wbHVnLmNhLnNhbnRpYS5nb3wHhcNOTgwNDAxMDAyOTIzWhcNMDAwMz
MxMD\
AyOTIzWjBfMQswCQYDVQQGEwJVUzEdMBsGA1UEChMURGllc2VsIENvbGxhYm9yYXRvcnkxDzAN
Bg\
NVBAsTBlNOTC1DQTEgMB4GA1UEAxMXZ2xvdy1wbHVnLmNhLnNhbnRpYS5nb3wgZ8wDQYJKo
ZIhv\
cNAQEBBQADgY0AMIGJAoGBAM5vxyzTTNVtEdFVS1Qnu5WXRnyxZ9RtvJQZslSRS5pG8kFi4VOYR
3\
5uOx+zjqVCaVwo+oIvKjiA2VbMe4VD5YFbxaVXmGnDDS5ct5hOh8ZSDnoOBy3dksKGkvJ8aEpOt1\
KBApx72sWL8Jp23wCFXMCc0hFehWW2rnhkxQQ3xM7dAgMBAAGjQjBAMB0GA1UdDgQWBBStil15p
3\
0BaWhh17Rh4lykOgWNVjAfBgNVHSMEGDAWgBStil15p30BaWhh17Rh4lykOgWNVjANBgkqhkiG9w\
0BAQQFAAOBgQAlVpDnEamYLuatyZ1xN9/q8Vf/lgoMV70Un4HYL6JvFdaDjREzzCuZLiMVUqeyN9\
oUYnAdqQ84vf4tP4mGcdq0RkG7SBaeRtMazwDfA2rLH49H+A4IVQjFjkArxg/QLa0tjVS/lkmDiV\
9A6kd+mxQb0xWohpG3QJJD7t/usI8f6g==\
-----END CERTIFICATE-----"

Identify directory servers for the CAs:

CertificateDirectory public ldap idcg-ds.lbl.gov
CertificateDirectory public ldap injector.ca.sandia.gov

Identify stakeholders and their certificate distribution agents:

UseConditionCAandIssuer
"/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=Srilekha Mudumbai Authority"

Akenti Application: Apache

UseCondRequired http://www-itg.lbl.gov/~mudumbai/Certificates

UseConditionCAandIssuer
"/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA"
"/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=Mary R. Thompson-sa3"

UseCondRequired http://www-itg.lbl.gov/~mrt/Certificates

Akenti Application: Apache

Use-conditions:

<HTML>
<TITLE> Use-Condition Certificate </TITLE>
<BODY>
-----BEGIN TEXT CERTIFICATE-----
-----BEGIN TEXT-----
use-condition
issuerAndCA
"/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence
Berkeley National Laboratory/OU=ICSD/CN=William E. Johnston sg1"

Identify what the use-condition is being imposed upon:

resource http://anl-hero.es.net/bwbroker

The policy model for this resource is hierarchical:

scope local

What is required:

attribute "(group : BWBROKER-ANL)"
enable access read,execute

Who can certify the attributes that satisfy this use-condition?

attributeIssuerAndCA
group "BWBROKER-ANL"
Attribute "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA"
"/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=William E. Johnston sg1"

Akenti Application: Apache

subjectCA "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA"

-----END TEXT-----

Assure that this certificate was issued by a legitimate stakeholder:

-----BEGIN SIGNATURE-----
v+TZtoZsyClhqTyXYY9/RmLHOfxY7nYewxuWJeBrT3sE/2F85jfuEHGRl/bBOz98
-----END SIGNATURE-----
-----END TEXT CERTIFICATE-----
</BODY>
</HTML>

Akenti Application: Apache

Attributes:

-----BEGIN TEXT ATTRIBUTE CERTIFICATE-----
attribute-certificate

What?

attribute group
value BWBROKER-ANL

When?

notValidBefore 980430233656Z
notValidAfter 980501003656Z

For whom?

subject "/C=US/O=Lawrence Berkeley National Laboratory/OU=ANL/UID=b30118/CN=Richard
Carlson/Email=racarlson@anl.gov" "/C=US/O=Lawrence Berkeley
 National Laboratory/OU=ICSD/CN=IDCG-CA"

By Whom?

issuer "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=William E. Johnston sg1"
"/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS
D/CN=IDCG-CA"

Guarantee:

-----BEGIN SIGNATURE-----
dxEqG/Hsj7s1V4Gu6YTmhuReLSjPcqy3h/nDsjX9+Mr4UyOyLMHEtbbkt3uBK/yT
-----END SIGNATURE-----

Akenti Access Control System

Authorization Certificates for GSS-API

The integration of Akenti with GSS uses the Simple Public-Key Management protocol (SPKM). (SPKM is one of several standard protocols defined to do session key management for GSS.)

If the resource server has multiple functions, then these functions may be individually access controlled by imposing use-conditions on named "actions."

If a hierarchical authority policy model is required for multiple stakeholders, then *.htauthority* files can be placed in a directory hierarchy that is available to the resource server (actually to Akenti).

Akenti Application: GSS API

Authorization Authorities (resource owner generated use-conditions)

Certification Authorities (identity - e.g. X.509)

Attribute Authorities (user characteristics)

certificate servers
- identity
- use-conditions
- attributes

(trusted agents of the signing authorities)

generate authoritative information

authorize

certificate cache manager
- cache all active certificates accounting for the cache time limits imposed by the stakeholders
- cache resource capabilities

policy engine
- identifies stakeholders
- acquires use-conditions
- identifies required attributes and issuers
- acquires attribute certificates
- validates certificates and matches use-conditions and attributes

stakeholder identities
- *.htauthority* files in directories corresponding to the authority hierarchy
- stakeholder DN
- stakeholder CA
- stakeholder directory server
- permitted user CAs

secure platform

auth. request   response ("denied" or a "capability")

user identity

operate

authorization request

user client application

Akenti/SPKM
- pass user identity and resource name to Akenti
- acquire capability from policy engine (or fail)
- do session key generation and exchange for GSS

secure channel (GSS)
- authenticated and/or confidential messaging

resource server
- the server associates "resource" identities with the directories where the htauthority files are kept

- the resource is accessed

11   **Akenti Integrated with the Generic Security Services API**

Akenti Access Control System

Authorization Certificates for CORBA

Two approaches to integration of Akenti and CORBA :

♦ **Use Akenti+SSL**
  • **coarse grained — only knows server identity, not functions**

♦ **Use OMG standard "intercepter" function**
  • **OID**
  • **user/client DN**

If the resource server has multiple functions, then these functions may be individually access controlled by imposing use-conditions on named "actions" that are derived from the OID.

If a hierarchical authority policy model is required for multiple stakeholders, then *.htauthority* files can be placed in a directory hierarchy that is available to Akenti.

Akenti Application: GSS API

Server

Akenti
- use-condition analysis based on
  - use name
  - object name
  - requested actions

"interceptor"
- A "request object" is supplied during SSL context establishment
- if callout to access control fails, the SSL connection fails

Client

ORB

ORB

SSL
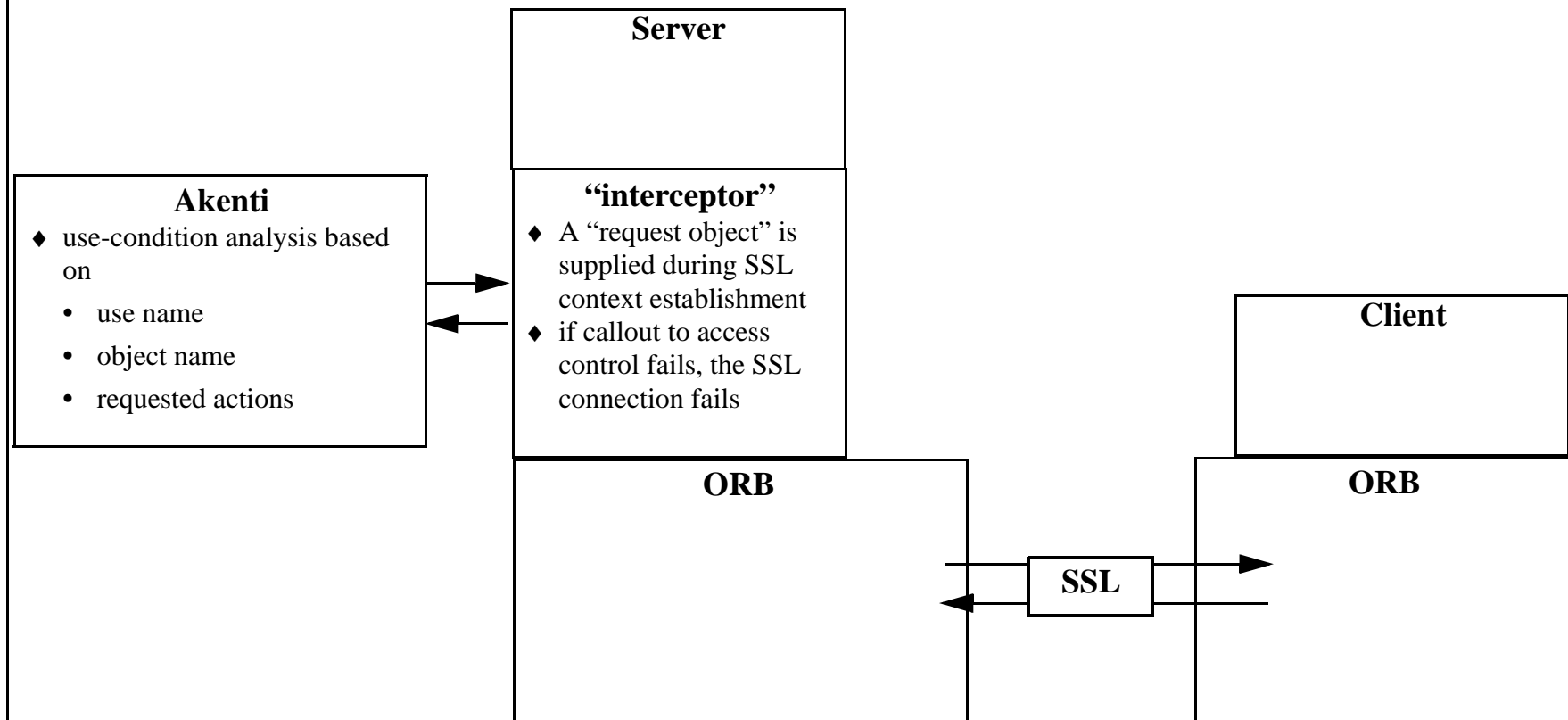
Akenti Access Control System

Certificate Infrastructure

How certificates are generated and managed is a key factor for the usability of the access control system:

- Must be very simple for the user
- Must be relatively simple for stakeholders
- Must not be an administrative burden

Netscape has built a useful collection of identity certificate management tools and user interfaces, and our implementation uses these facilities.

This section presents a summary of material that may be found at http://www-itg.lbl.gov/security/Akenti

- User Interaction
- Identity establishment
- Use-Condition generation
- Attribute Generation

User Interaction

The normal user interaction is intended to be as transparent as possible. When attempting to access a secure resource, the user client (e.g. a Web browser) supplies the private key to authenticate the user. The access control system identifies and obtains all of the required certificates: use-conditions for the resource and the corresponding user attributes. When the use-conditions are satisfied and the user identity authenticated, access is permitted with no user action other than making the private key available.

7-UI3   8-UI4   9-UI5

Akenti: Certificate Infrastructure

LBL Data Intensive Distributed Computing Research Group and Imaging

File Edit View Go Communicator Help

Back Forward Reload Home Search Guide Print Security Stop

Bookmarks Location: http://www.itg.lbl.gov/

Instant Message Internet Lookup New&Cool

Data Intensive Dist
Computing Research
and
Imaging and Distri
Collaboration Gr

NERSC and
Information and Computing Science:
Ernest Orlando Lawrence Berkeley
One Cyclotron Road, 50B-2270, B

This page summarizes the activities c
Collaboration Group. A marker like this ☒ indicates that within one or two hops you'll find an **interactive** resource like the
Whole Frog Project where you can experience the benefits that imaging and networking bring to science, education, and
industry.

Open Page

Enter the World Wide Web location (URL) or specify the local file you would
like to open:

https://imglib.lbl.gov/shared   Choose File...

Open location or file in: ○ Composer   Open   Cancel   Help
                           ● Navigator

Access a secure server.

_____

**Secure Web servers use the SSL
(Secure Sockets Layer) protocol to
authenticate the client and the
server, and for setting up an
encrypted communication channel.
https refers to Web servers that use
the SSL protocol. In this case, access
control is provided by Akenti.**

Akenti: Certificate Infrastructure

ve Distributed Computing Research Group and Imaging and Distributed Collaboration Gr -

Communicator Help

Reload Home Search Guide Print Security Stop

Location: http://www.itg.lbl.gov/

Internet Lookup New&Cool

Data Intensive Distributed Computing Research Group *and* Imaging and Distributed

Password Entry Dialog

Please enter the password or the pin for Communicator Certificate DB.

`*************`

OK   Cancel

Computing Scien
awrence Berkel
oad, 50B-2270, Berkeley, CA, USA 94720

rizes the activities of the Data Intensive Distributed Computing Research Group and I
oup. A marker like this indicates that within one or two hops you'll find an **interac**

Make your identity available for authentication.

_____

When a remote server requests your identity you must "unlock" your private key so that it may be used to authenticate your identity. (Recall that your identity is authenticated by checking that your private key and your published public key match.) Netscape allows several options for when your passphrase is requested, but at the very least it is always requested the first time that you are authenticated.

Akenti: Certificate Infrastructure
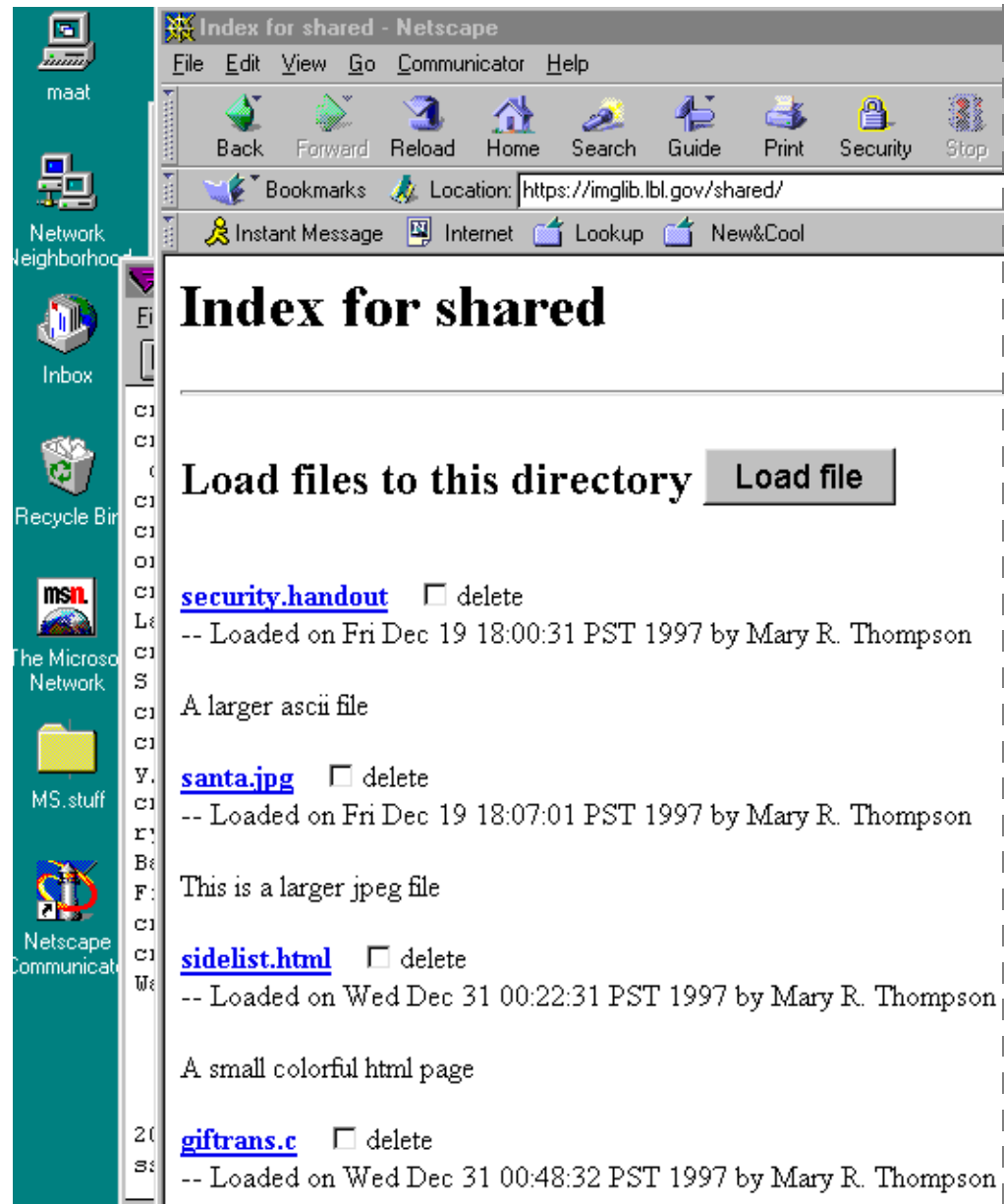
The user has met the use-conditions for this resource and access is allowed.

The "normal" operation of the access control system is intended to be transparent to the user, and specific use-conditions are not normally visible to the user. The use-conditions, and the user attributes needed to satisfy them, are established elsewhere. (However if "real" credentials beyond identity are required for a particular resource, then the user will have to provide those to the party who is certifying that user attribute.)

Identity Establishment

An identity certificate binds a user name to a public key in a document issued by a trusted third-party (the Certification Authority.) The private key and the public key are cryptographically bound - what one encrypts only the other can decrypt. It is this binding that allows the private key - if it has been held in confidence by its owner - to strongly authenticate the owner to anyone who obtains the owner's public key from the CA.

4   5

Akenti: Certificate Infrastructure

Netscape: Netscape Certificate Service Menu

File   Edit   View   Go   Bookmarks   Options   Directory   Window

Back   Forward   Home   Reload   Images   Open   Print   Find   Stop

Netsite: https://idcg-ca/

What's New?   What's Cool?   Destinations   Net Search   People   Software

NETSCAPE CERTIFICATE SERVER

NETSCAPE CERTIFICATE SERVER

Public   Privileged

Public Menu

Request a Personal Certificate

Request a Server Certificate

Search for Certificates

List Certificates

Accept This Authority in Your Navigator

Accept This Authority in Your Server

Review Certificate Revocation List

Welcome to the Netscape Certificate Server! The certificate server allows you to create, sign, and man certificates.

The left frame in this window displays a menu of operations that you can perform. There are two menus

- **Public Menu.** If you need to request a certificate, search for certificates, trust a certificate authority, or review a certificate revocation list, use the operations available in the Public Menu.

  To access the Public Menu of operations, click the **Public** button.

- **Privileged Menu.** If you work for this certificate authority as an issuing agent or administrator, and you need to issue certificates, revoke certificates, or update the certificate revocation list or the directory server, use the operations available in the Privileged Menu.

The Certification Authority issues identity certificates to users.

_____

The CA will have a published policy on what is required of the user in order to receive a certificate. The request is received by the CA administrator and held until the identity verification process has been completed.

Imaging and Distributed Computing Group,
Information and Computing Sciences Division

[Global.Capability.Akenti.summary.VG.fm - July 22, 1998]
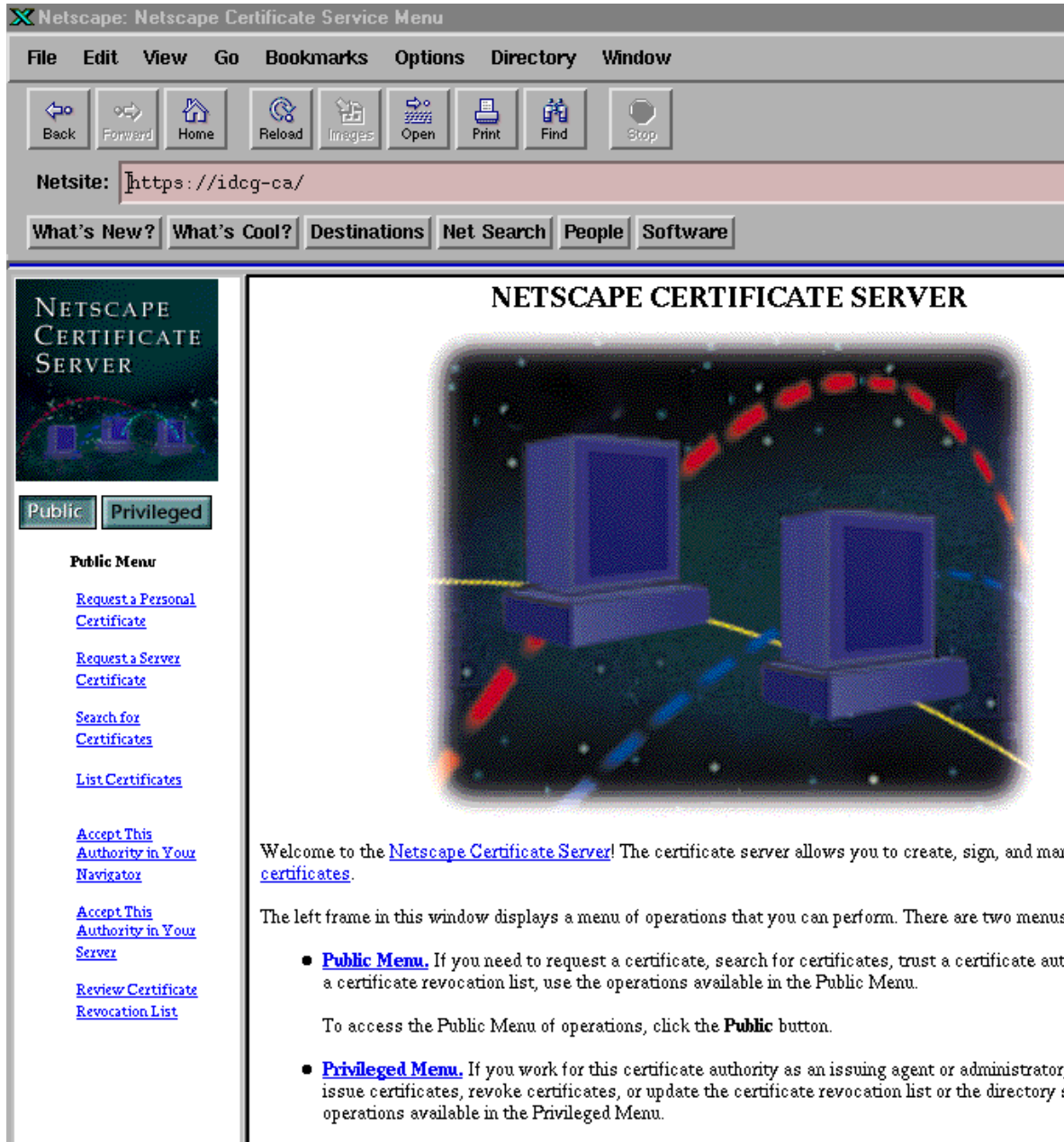
Akenti: Certificate Infrastructure

The user supplies the basic information for a certificate

_____

"Your Full Name" becomes your "Common Name" in the X.509 certificate. If the same CA issues you multiple certificates, then the names must be unique.

The exact form of "Org. Unit", "Org.", and "Country" must be obtained from the CA administrator.

Akenti: Certificate Infrastructure

Use-conditions

A resource stakeholder (e.g. data "owner") will impose use-conditions that must be met before access is allowed. Akenti provides several forms of use-conditions. Example use-conditions:

♦ Some component of an X.509 certificate (e.g. "organization" - fairly general or "common name" - very specific)
(in this case the X.509 certificate supplies all of the required attributes)

♦ Group membership
(stakeholders can establish their own groups, and attribute certificates issued by parties named by the stakeholder will place a user into the group - i.e., an attribute certificate issued to a user that attests to membership in the group)

12

Akenti: Certificate Infrastructure

The completed use-condition certificate (requiring an X.509 component in this case) is signed by the stakeholder and made available by a trusted server.

Attributes

Attributes are provided by certifiers trusted by the use-condition issuer. Formally, attributes are associated with users, not with resources. (Though specific groups may be associated with specific resources.)

12   13

**Imaging and Distributed Computing Group,
Information and Computing Sciences Division**

[Global.Capability.Akenti.summary.VG.fm - July 22, 1998]

Akenti: Certificate Infrastructure

Preview and Generate Attribute Certificate

Preview the requirements for generating an attribute certificate and if satisfied, sign it.

Attribute	group
Value	HPSS
SubjectAndCA	Mary R. Thompson , IDCG-CA
AttributeIssuerAndCA	William E. Johnston sg1 , IDCG-CA

Cancel   < Back   Sign Certificate

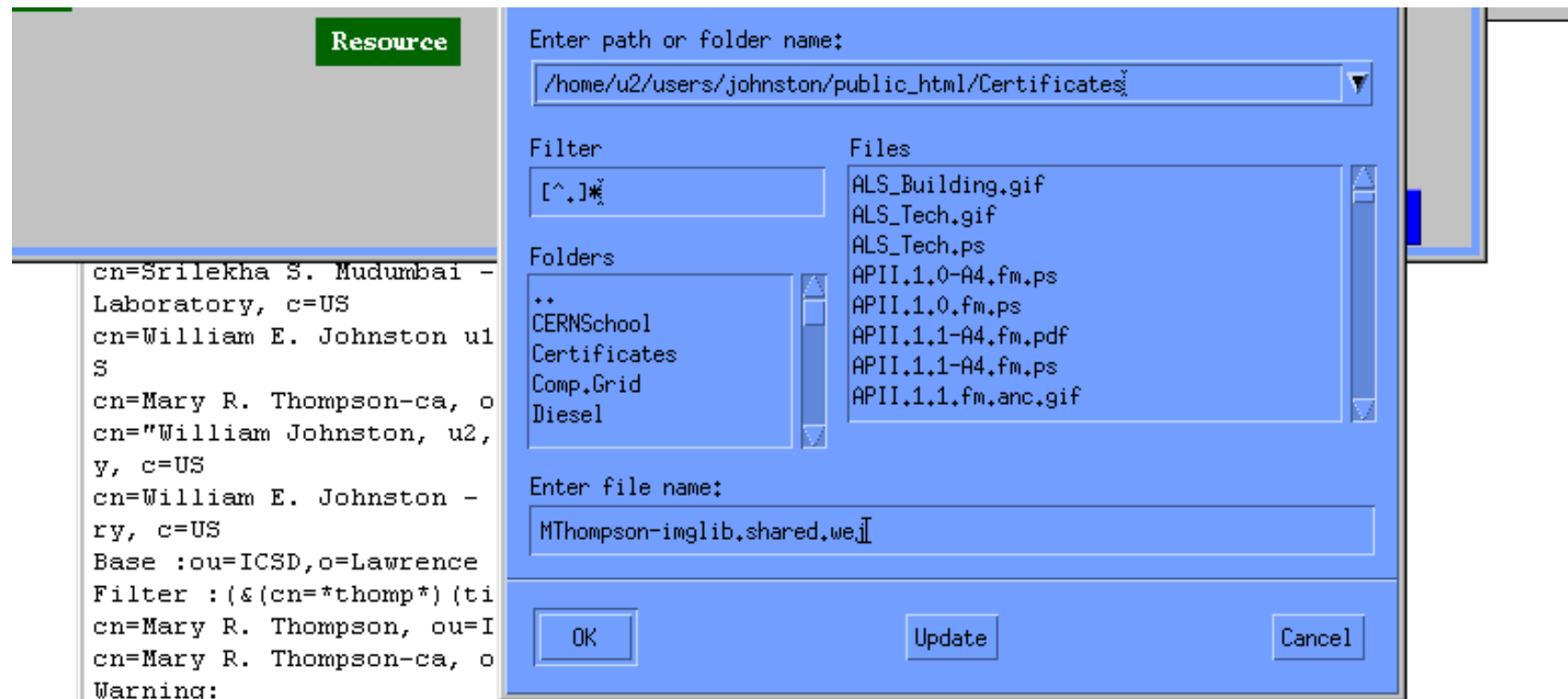## The attribute certificate is constructed and signed.
_____

Akenti: Certificate Infrastructure

The certificate is "published".

_____

The location of attribute certificates is an important part of the assurance process. The signing authority must designate one or more trusted servers for publishing attribute certificates. These servers are "trusted" not because a certificate can be counterfeited (extremely difficult - impossible with ordinary resources - because of the cryptographic strength of public-key cryptography) but because the absence of a certificate from the designated server (usually the certifier's Web server) denies access to a user.
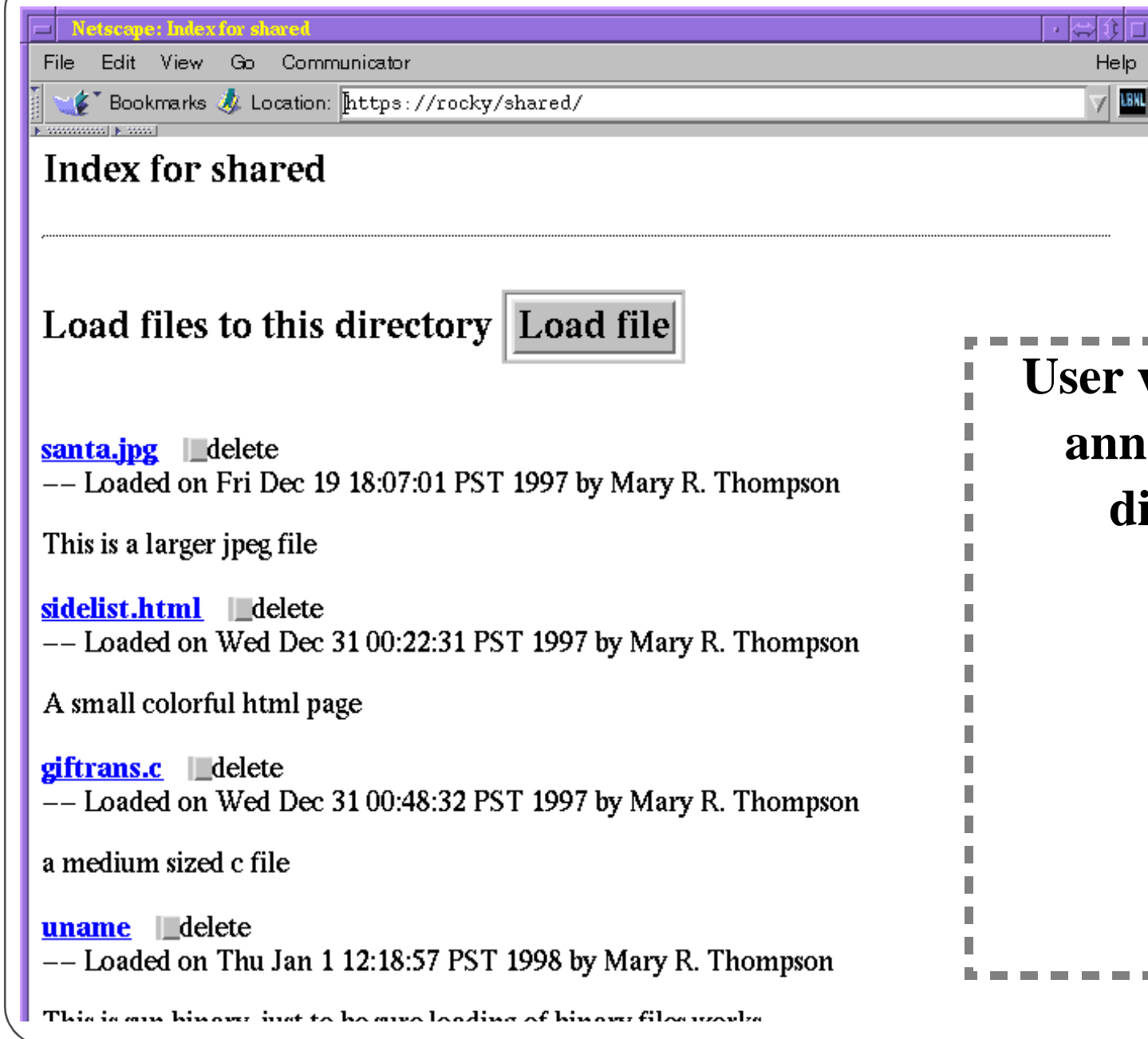
CDS: A Simple Akenti Application

CDS (access *Controlled Data Sharing)* provides a simple interface for uploading and downloading files to and from an area of a server that is access controlled by use-condition certificates.

The file appears on a Web page, and may be described by a simple annotation.

The goal is a secure and easily used, group-oriented, data sharing facility.

Akenti: Application

Netscape: Index for shared

File   Edit   View   Go   Communicator   Help

Bookmarks   Location: https://rocky/shared/

Index for shared

_____

Load files to this directory [Load file]

santa.jpg   ▢delete
–– Loaded on Fri Dec 19 18:07:01 PST 1997 by Mary R. Thompson

This is a larger jpeg file

sidelist.html   ▢delete
–– Loaded on Wed Dec 31 00:22:31 PST 1997 by Mary R. Thompson

A small colorful html page

giftrans.c   ▢delete
–– Loaded on Wed Dec 31 00:48:32 PST 1997 by Mary R. Thompson

a medium sized c file

uname   ▢delete
–– Loaded on Thu Jan 1 12:18:57 PST 1998 by Mary R. Thompson

This is sun binary, just to be sure loading of binary files works

> **User view of CDS annotated file directory.**

Akenti: Application

File   Edit   View   Go   Communicator   Help

Bookmarks   Location: https://rocky/shared/setup.cgi

Debugging output for shared–setup /C=US/O=Lawrence Berkeley National
Laboratory/OU=ICSD/UID=mrt/CN=Mary R. Thompson/Email=mrthompson@lbl.gov
has rights: read,write

Akenti access check for /shared

The identity

C=US
O=Lawrence Berkeley National Laboratory
OU=ICSD
UID=mrt
CN=Mary R. Thompson
Email=mrthompson@lbl.gov

has rights: **read,write**
In directory **/shared**

The user can query the current access rights.

Akenti: Application

Netscape: setup shared files

File Edit View Go Communicator   Help

Bookmarks   Location: https://131.243.2.48/shared/setup.cgi?dir_name=shared&action=Load

Debugging output for shared–setup /C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/UID=mrt/CN=Mary R. Thompson/Email=mrthompson@lbl.gov has rights: read,write

LBNL Image Library –– Upload a file

Destination directory name | shared
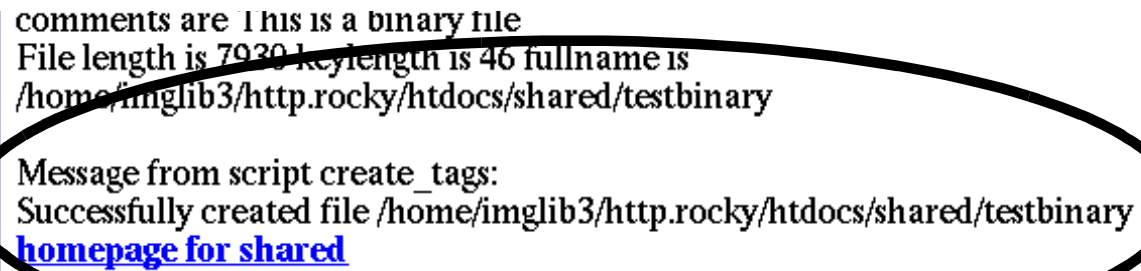
Destination file name | testbinary

Enter any comments about this file:

    This is a binary file

Path name of source file: | in/solaris/mbone_vcr | Browse...

send_file

Upload is intended to be simple, and provides for free-form user description of the file.

Imaging and Distributed Computing Group, Information and Computing Sciences Division

[Global.Capability.Akenti.summary.VG.fm - July 22, 1998]

Akenti: Application

comments are This is a binary file
File length is 7930 keylength is 46 fullname is
/home/imglib3/http.rocky/htdocs/shared/testbinary

Message from script create_tags:
Successfully created file /home/imglib3/http.rocky/htdocs/shared/testbinary
homepage for shared

Filtering the audit log will provide user feedback.

Akenti: Application

Load files to this directory [Load file]

santa.jpg ☐delete
–– Loaded on Fri Dec 19 18:07:01 PST 1997 by Mary R. Thompson

This is a larger jpeg file

sidelist.html ☐delete
–– Loaded on Wed Dec 31 00:22:31 PST 1997 by Mary R. Thompson

A small colorful html page

giftrans.c ☐delete
–– Loaded on Wed Dec 31 00:48:32 PST 1997 by Mary R. Thompson

a medium sized c file

uname ☐delete
–– Loaded on Thu Jan 1 12:18:57 PST 1998 by Mary R. Thompson

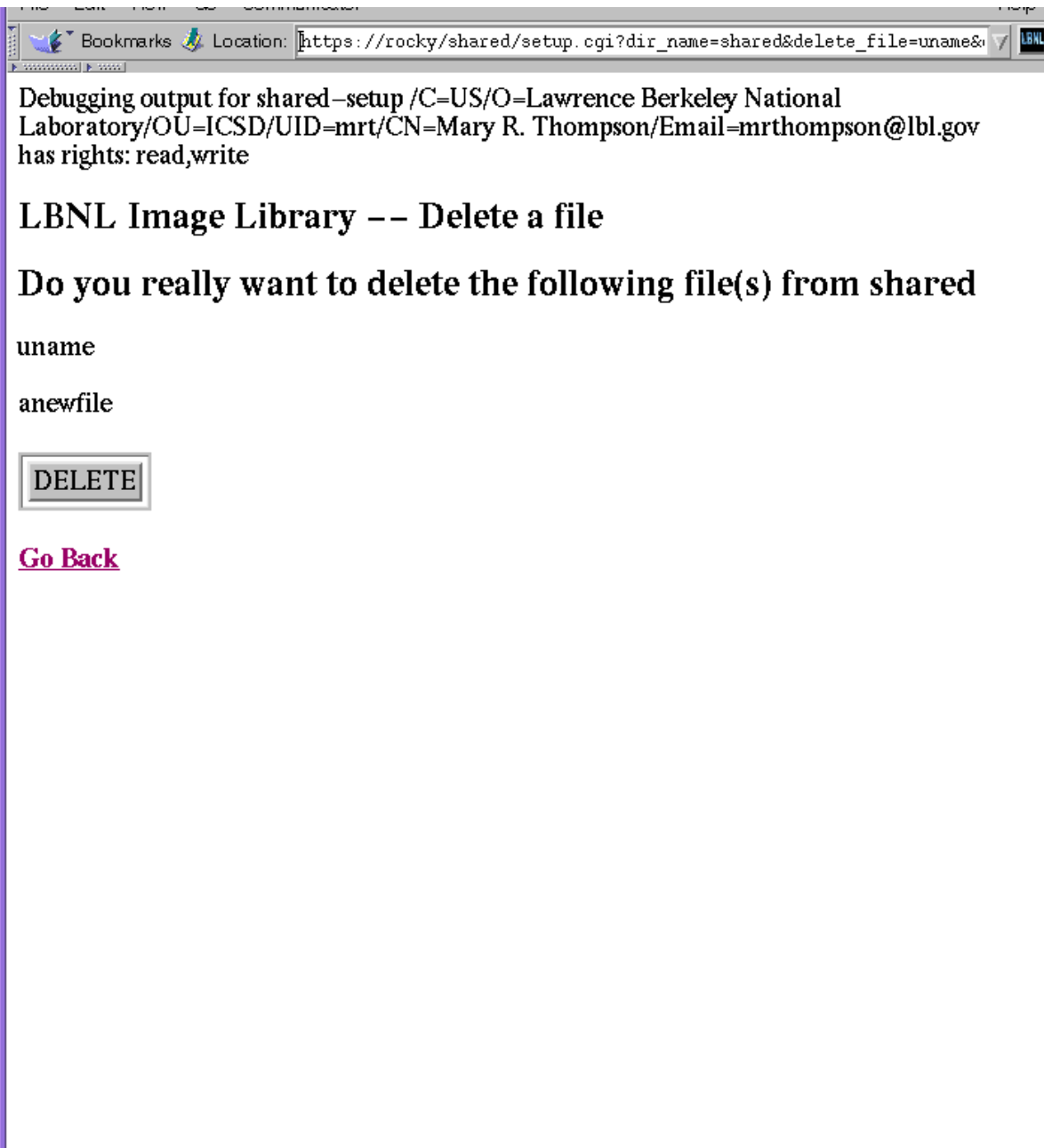This is sun binary, just to be sure loading of binary files works

anewfile ☐delete
–– Loaded on Tue Jan 6 12:19:09 PST 1998 by Mary R. Thompson

loaded just to the experimental akenti system

testbinary ☐delete
–– Loaded on Mon Jan 12 17:22:34 PST 1998 by Mary R. Thompson

This is a binary file

[Delete selected files]

A new shared file has been created.

Akenti: Application

Bookmarks | Location: https://rocky/shared/setup.cgi?dir_name=shared&delete_file=uname&

Debugging output for shared–setup /C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/UID=mrt/CN=Mary R. Thompson/Email=mrthompson@lbl.gov has rights: read,write

LBNL Image Library –– Delete a file

Do you really want to delete the following file(s) from shared

uname

anewfile

DELETE

Go Back

Delete capability is granted separately from access.

Akenti: Application

File   Edit   View   Go   Communicator   Help

Bookmarks   Location: https://131.243.2.48/shared/.htauthority

```
CertificateDirectory public web george
CertificateDirectory public ldap idcg-ds.lbl.gov
CertificateDirectory trusted file /home/u2/users/mudumbai/Newce
UseConditionCAandIssuer "/C=US/O=Lawrence Berkeley National Lab/OU=ICSD/CN=Srilekha Mudumbai Authority"
UseConditionCAandIssuer "/C=US/O=Lawrence Berkeley National Lab/OU=ICSD/CN=Mary R. Thompson-sal"
UseCondRequired http://www-itg.lbl.gov/~mudumbai/Certificates/r
```

Users will be able to query who defines use-conditions, but not the specific use-condition.

Bandwidth Reservation

We propose a model for bandwidth reservation that can be used in the context of a general resource reservation scheme, but at the same time stay within the scalable model of the differentiated classes of service as described in the IETF diffserv Working Group documents ([5]).

The basic idea is to have bilateral end node agreements that "reserve" bandwidth in the sense that a site actively manages allocation against one or more classes of service. The overall limits on a class of service are established in the corresponding service-level agreement between the institution of the end nodes and the ISP, but the allocation of flows to this class is closely managed by the end node institutions at the site egress.

Further, the resource allocation should be policy based in a way that allows automated reservation, and it should also be possible to proxy one's policy based authority to another site so that the bilateral agreements necessary for inter-site application operation happen automatically. (See, e.g., [2].)

The network level technology to accomplish this is provided by the classifier/shaper/policer functions of the diffserv "traffic conditioner" (TC) element. Layered on top of the TC is a "slot" allocation mechanism ("bandwidth manager") that manages the use of a service class. When instantiated, this slot is a "micro flow" in the diffserv terminology.

Reservation requests are made to the bandwidth manager. The identity of the requestor (user_A), together with the requested resource (time slot, source id, bandwidth) are compared with policy. If the requestor and resource meet the policy, a reservation is made (the slot is allocated and the available bandwidth in the SLA is decremented) and a certificate (a digitally signed document) is issued by the bandwidth manager to represent the reservation.
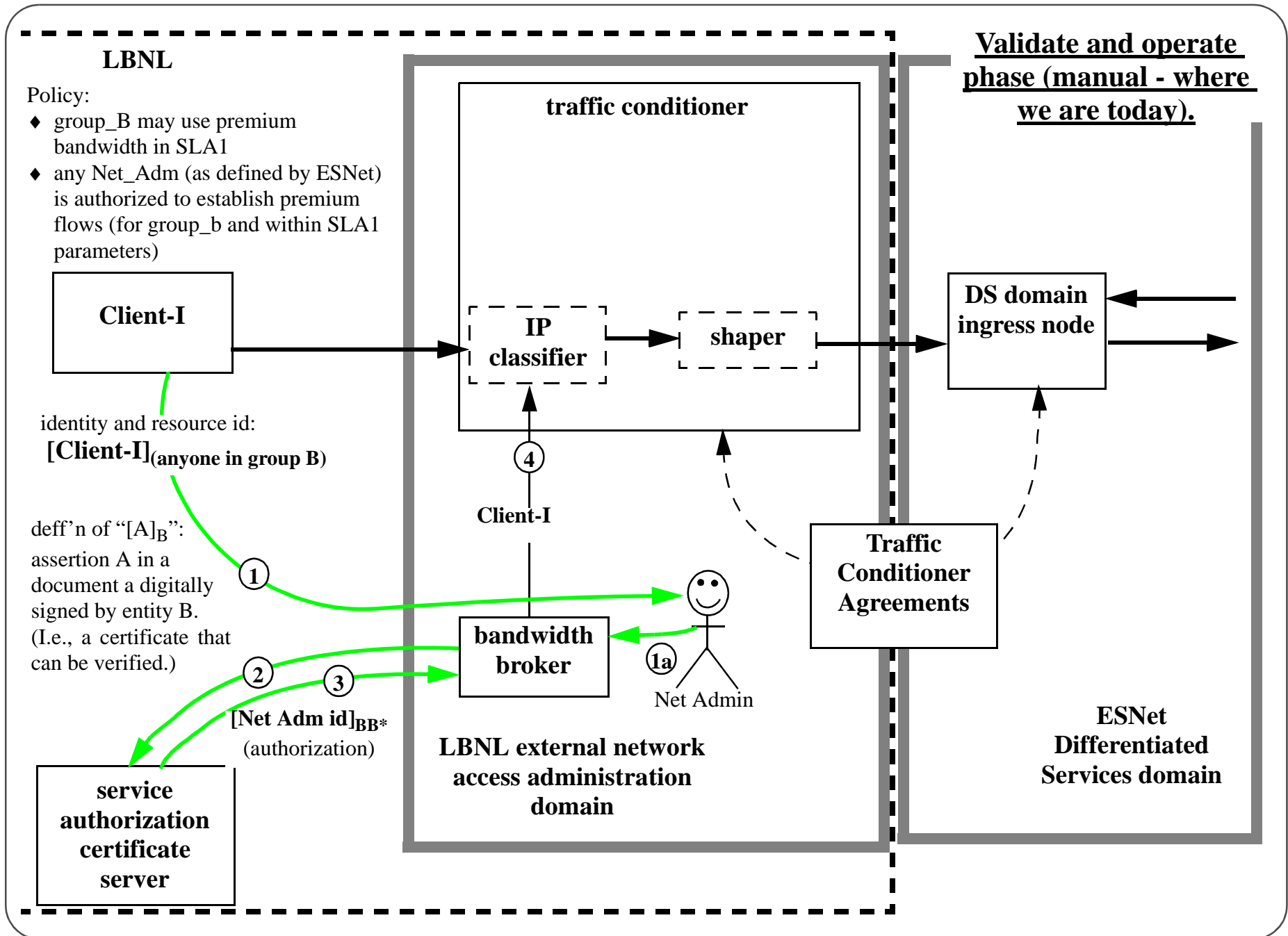
When, at some point in the future, a request is made to instantiate the flow (i.e. start the instrument or application) the bandwidth manager retrieves the certificate (based on the requestor id and flow characteristics), validates the user and certificate, and instantiates the flow.

The flow characteristics are passed to the TC for classification and enforcement. From the point of view of the ingress router of the ISP, the SLA is never violated because the site bandwidth manager does not over allocate and the TC enforces flow characteristics as reserved.

Another important component in this architecture is a bandwidth broker. This service interacts with the bandwidth manager at the target site in order to accomplish the bilateral reservation. The model here is that some entity ("user_B") at the target site ("site_B") is the (willing) receiver of the flow. The site_B entity must have the right (i.e., be within the policy of site_B) to utilize this flow. User_B conveys (a priori) its authority (in the form of a proxy certificate) to user_A, and the site_A bandwidth broker presents this proxy to the site_B bandwidth manager in order to accomplish the reservation. The site_B incoming flow could probably just be authenticated based on the flow spec matching the reservation (i.e., site_B trusts site_A to authenticate the flow when it is instantiated), although more elaborate authentication is possible.

Akenti Application: Bandwidth Reservation

LBNL

Policy:
- group_B may use premium bandwidth in SLA1
- any Net_Adm (as defined by ESNet) is authorized to establish premium flows (for group_b and within SLA1 parameters)

Validate and operate phase (manual - where we are today).

Client-I

identity and resource id:
[Client-I]$_{(anyone in group B)}$

deff'n of "[A]$_B$":
assertion A in a document a digitally signed by entity B. (I.e., a certificate that can be verified.)

traffic conditioner

IP classifier → **shaper**

DS domain ingress node

④

Client-I

①

② ③

bandwidth broker

1a

Traffic Conditioner Agreements

Net Admin

[Net Adm id]$_{BB*}$
(authorization)

LBNL external network access administration domain

service authorization certificate server

ESNet Differentiated Services domain

Akenti Application: Bandwidth Reservation

service authorization certificate server

[Client-II]$_{(anyone\ in\ ALS)}$

[Client-I]$_{(anyone\ in\ group\ B)}$

Premium bandwidth request, policy-based authorization, and reservation phase (automated).

① $r_1 \subset$ SLA-1

⑥

$r_2 \subset$ SLA-3

[AuC]$_{BB}$

①

⑥

RSL request

------

co-allocator (multi-resource broker)

⑥

GRAM

local policy authorizer

②

bandwidth broker

③

④ ⑤

LBNL external network access administration domain

Service Class pool manager

policy (expressed by a human authority and automatically checked):

♦ **SLA-1** is a high throughput service level and is restricted to:
   i) person A,
   ii) those members of group B who are LBNL employees and are using systems in the Clipper sub-domain.
   • **SLA-1** requires
   (subject CN=A or (group=B and O=LBL and DNS=clipper.lbl.gov))

♦ **SLA-2** is the default class of service for LBNL, however LBNL routes for MSRI which does not get this class.
   • **SLA-2** requires O=LBL

♦ **SLA-3** is a special class of service negotiated between LBNL, ESNet and the ALS
   • **SLA-3** requires O=LBL, OU=ALS

Authorization certificate ("AuC")
 (the result of a policy-based decision to permit the use of this class of service)
class = SLA-1
authorized =
((X.509@LBL-ca.lbl.gov:CN=A)
OR
(group=B@domain_A and
 X.509@LBL-ca.lbl.gov:O=lbl.gov AND
 DNS=clipper.lbl.gov))
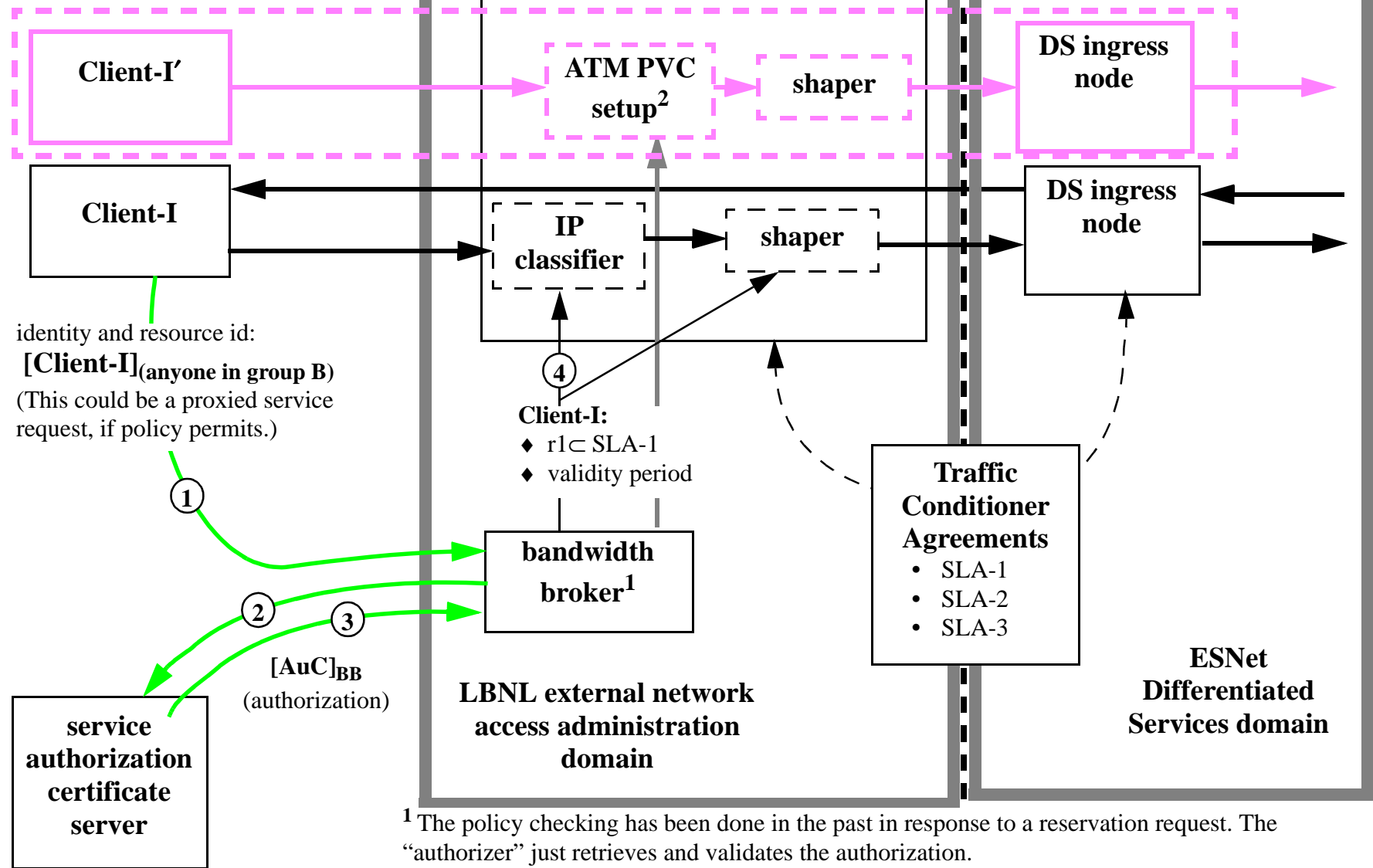*validity times = hour1:day1 - hour2:day2*
signed = [message digest]$_{BB}$

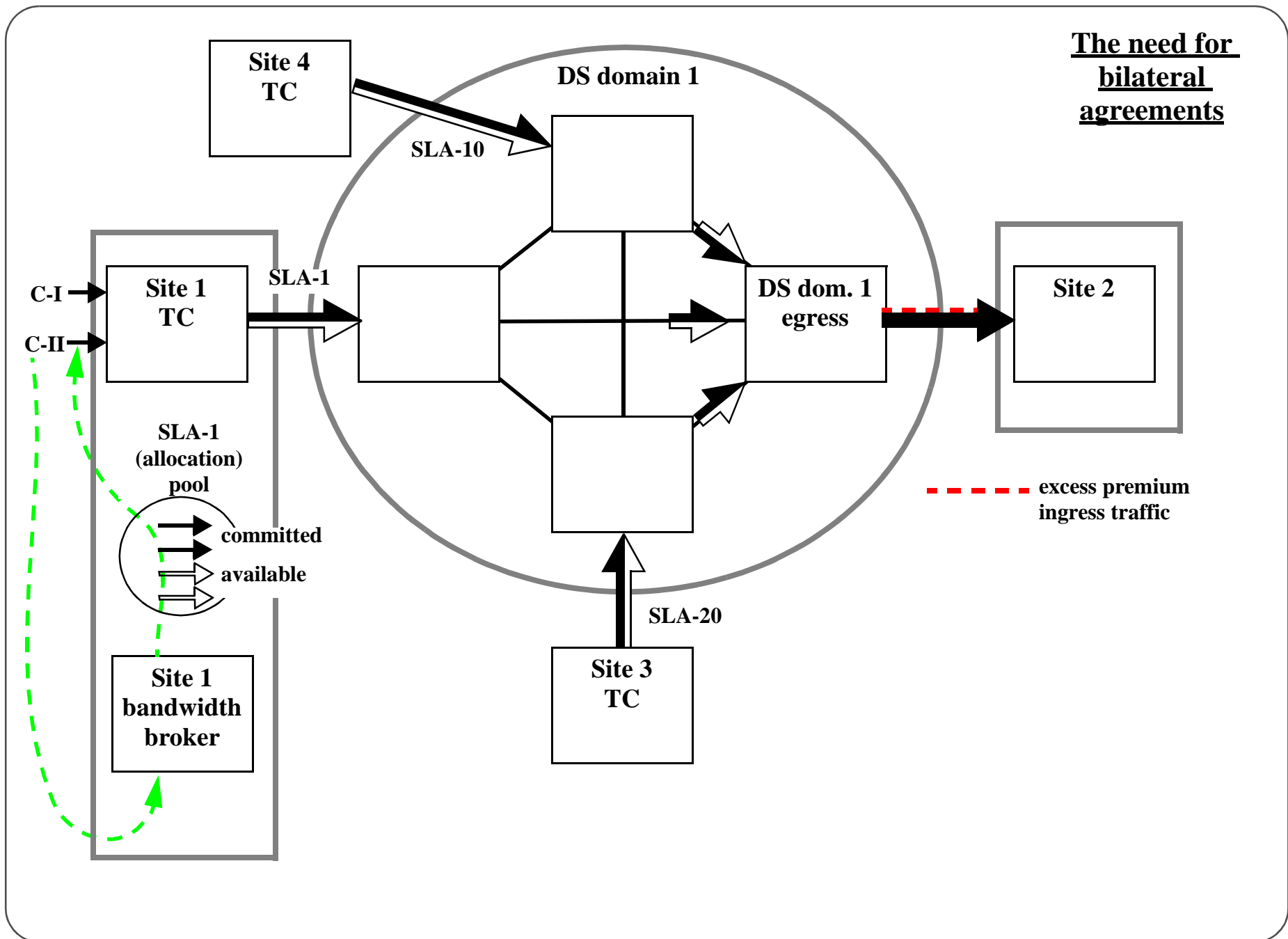$\Rightarrow$ **Globus resource allocation mechanisms**

Akenti Application: Bandwidth Reservation

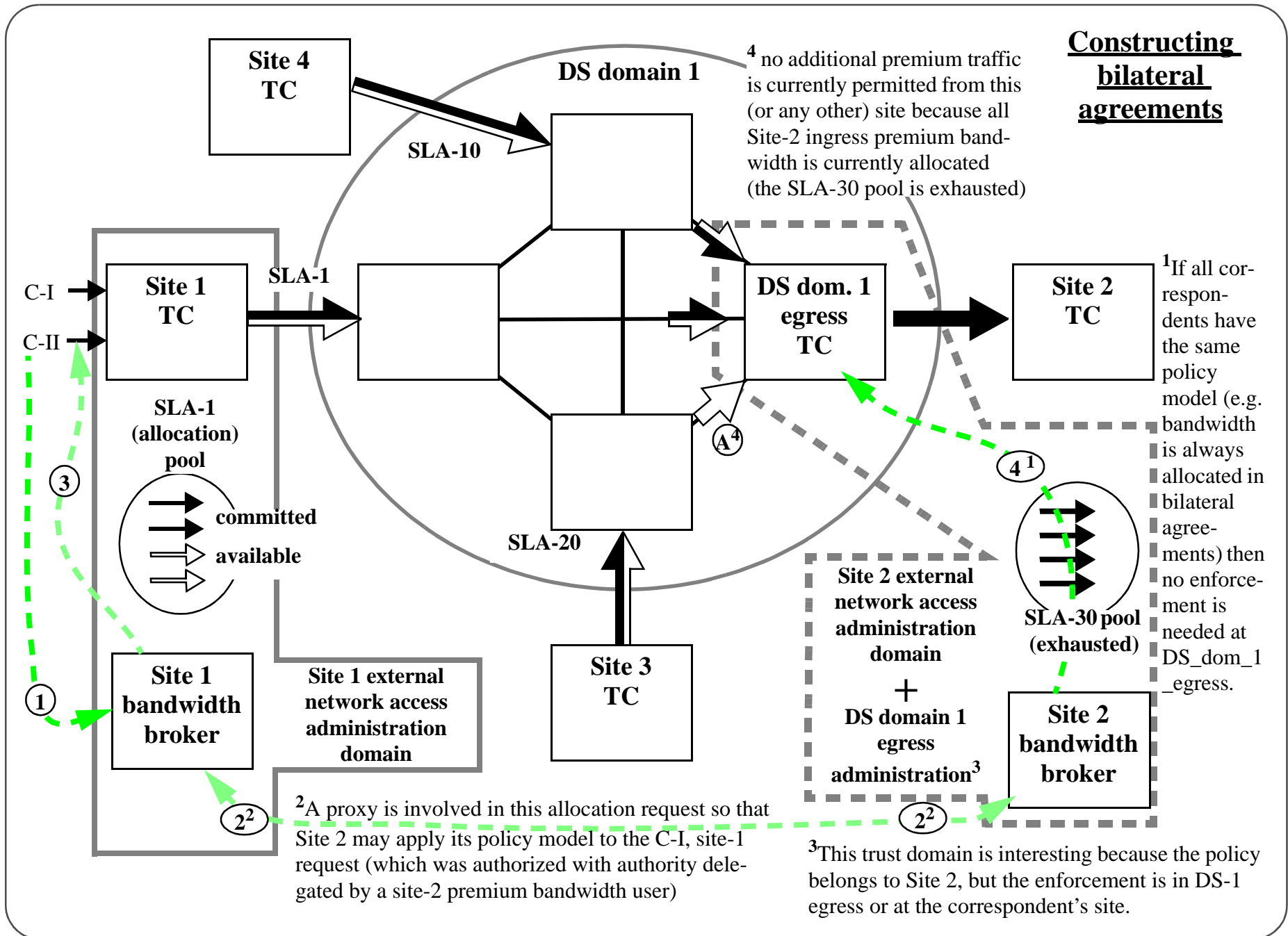[2]A very similar model could be used to implement "morphnet".

Validate and operate phase (automated).

traffic conditioner

Client-I′

ATM PVC setup[2]

shaper

DS ingress node

Client-I

DS ingress node

IP classifier

shaper

identity and resource id:

[Client-I]$_{(anyone\ in\ group\ B)}$

(This could be a proxied service request, if policy permits.)

4

Client-I:
- r1 ⊂ SLA-1
- validity period

1

2   3

bandwidth broker[1]

Traffic Conditioner Agreements
- SLA-1
- SLA-2
- SLA-3

[AuC]$_{BB}$
(authorization)

service authorization certificate server

LBNL external network access administration domain

ESNet Differentiated Services domain

[1] The policy checking has been done in the past in response to a reservation request. The "authorizer" just retrieves and validates the authorization.

Akenti Application: Bandwidth Reservation

Site 4 TC

DS domain 1

SLA-10

The need for bilateral agreements

C-I

C-II

Site 1 TC

SLA-1

DS dom. 1 egress

Site 2

SLA-1 (allocation) pool

committed

available

Site 1 bandwidth broker

SLA-20

Site 3 TC

- - - excess premium ingress traffic

Akenti Application: Bandwidth Reservation

Constructing bilateral agreements

Site 4 TC

DS domain 1

SLA-10

[4] no additional premium traffic is currently permitted from this (or any other) site because all Site-2 ingress premium bandwidth is currently allocated (the SLA-30 pool is exhausted)

C-I

C-II

Site 1 TC

SLA-1

DS dom. 1 egress TC

Site 2 TC

[1] If all correspondents have the same policy model (e.g. bandwidth is always allocated in bilateral agreements) then no enforcement is needed at DS_dom_1_egress.

SLA-1 (allocation) pool

committed

available

A[4]

4 [1]

SLA-30 pool (exhausted)

SLA-20

Site 3 TC

Site 2 external network access administration domain

+

DS domain 1 egress administration[3]

(3)

(1)

Site 1 bandwidth broker

Site 1 external network access administration domain

Site 2 bandwidth broker

2[2]

[2] A proxy is involved in this allocation request so that Site 2 may apply its policy model to the C-I, site-1 request (which was authorized with authority delegated by a site-2 premium bandwidth user)

2[2]

[3] This trust domain is interesting because the policy belongs to Site 2, but the enforcement is in DS-1 egress or at the correspondent's site.

Monitoring

The NetLogger [1] event monitoring system is being used to track and record all "events" — acquisition of policy "elements," and their corresponding certificates.

Imaging and Distributed Computing Group,
Information and Computing Sciences Division

[Global.Capability.Akenti.summary.VG.fm - July 22, 1998]

Akenti Application: Monitoring

Akenti access check for http://imglib.lbl.gov/shared/wej

The identity
/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/UID=wej/CN=William E. Johnston/Email=wej@george.lbl.gov

has rights: **none**

LogFile

STATUS PANELS:

Collecting policy elements ...

Validating use conditions ...

Satisfying access use conditions ...

Previous Message   Next Message

*** HELP ***

DIRECTORY SERVICES:

Resource=/home/imglib3/http.imglib/htdocs/shared/wej/
    CertificateDirectory: public ldap idcg–ds.lbl.gov
    CertificateDirectory: trusted file /home/u2/users/johnston/public_html/

Resource=/home/imglib3/http.imglib/htdocs/shared/
    CertificateDirectory: public ldap idcg–ds.lbl.gov
    CertificateDirectory: trusted file /home/u2/users/mudumbai/Newcerts
    CertificateDirectory: trusted file /home/u3/users/mrt/public_html/Attrib

Resource=/home/imglib3/http.imglib/htdocs/
    CertificateDirectory: public ldap idcg–ds.lbl.gov

User-level Access Checking.

**(An Applet invoked from an access controlled Web server.
Even to get this, the user must have an identity certificate
from a trusted CA.
Each colored box results from analyzing a policy element.
The corresponding certificates are displayed on the right.
Clicking on the box will show the policy element.)**

Akenti Application: Monitoring

Akenti policy files for http://imglib.lbl.gov/shared/wej

The identity
/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/UID=wej/CN=William E. Johnston/Email=wej@george.lbl.gov

has the rights: **none**

The policy file for **shared/wej** is:

CertificateDirectory public ldap idcg-ds.lbl.gov
CertificateDirectory trusted file /home/u2/users/johnston/public_html/Certificates
UseConditionCAandIssuer "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley National La
sgl"
UseCondRequired http://www-itg.lbl.gov/~johnston/Certificates/

Pulling UseConditionCertificate http://www-itg.lbl.gov/~johnston/Certificates/
reqstr is: GET /~johnston/Certificates/ HTTP/1.0
Pulling UseConditionCertificate http://www-itg.lbl.gov/~johnston/Certificates/4025b262.0
reqstr is: GET /~johnston/Certificates/4025b262.0 HTTP/1.0

Use Condition Certificate is:

-----BEGIN TEXT CERTIFICATE-----
-----BEGIN TEXT-----
use-condition
issuerAndCA "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley National Laboratory/OU=I
attribute "(group : HPSS)"
resource http://imglib.lbl.gov/shared/wej
scope sub-tree
enable access read,write,modify,chmod
subjectCA "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA"
attributeIssuerAndCA group Attribute "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley N
Johnston sgl"
-----END TEXT-----
-----BEGIN SIGNATURE-----
0IIsQ53O94OPX1/+dv8IwjQxf6MVntZRxeduGWsvaJSnP2RpHTgsYXayIn5EFI
-----END SIGNATURE-----
-----END TEXT CERTIFICATE-----

Administrator-level Policy Checking.

(Essentially a real-time display of the Akenti log.)

Imaging and Distributed Computing Group,
Information and Computing Sciences Division

[Global.Capability.Akenti.summary.VG.fm - July 22, 1998]

Akenti Application: Monitoring

The policy file for **shared** is:

#CertificateDirectory public web george
CertificateDirectory public ldap idcg-ds.lbl.gov
CertificateDirectory trusted file /home/u2/users/mudumbai/Newcerts
CertificateDirectory trusted file /home/u3/users/mrt/public_html/Attributes
UseConditionCAandIssuer "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley National La
OR "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=
UseCondRequired http://www-itg.lbl.gov/~mrt/Certificates/

Pulling UseConditionCertificate http://www-itg.lbl.gov/~mrt/Certificates/
reqstr is: GET /~mrt/Certificates/ HTTP/1.0
Pulling UseConditionCertificate http://www-itg.lbl.gov/~mrt/Certificates/68c2edd0.0
reqstr is: GET /~mrt/Certificates/68c2edd0.0 HTTP/1.0

Use Condition Certificate is:

-----BEGIN TEXT CERTIFICATE-----
-----BEGIN TEXT-----
use-condition
UID "rocky.lbl.gov#68c2edd0#Wed Jun 10 14:16:35 PDT 1998"
issuerAndCA "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley National Laboratory/OU=I
resource http://imglib.lbl.gov/shared
scope sub-tree
attribute "(group : IDCG)"
enable read,write,modify,chmod
attributeIssuerAndCA group "IDCG" Attribute "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Be
R. Thompson-sa"
subjectCA "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA"
subjectCA "/C=US/O=Diesel Combustion Collaboratory/OU=SNL/CN=DieselCert.ca.sandia.gov"
-----END TEXT-----
-----BEGIN SIGNATURE-----
T7lUPPGkqvAheIeFXLa4Neppp2Q2mijx+ZCGI2A2AjixfuLMgzfYs0ViLXUsLriptJRYDDKHUQ6h
947FIkBmSpzehMbd3L6jgerP0vISxJ/VrcfNY5UZBdHWSq8ITyTbxEoflcz+cmqvxgIBmIhk5HW/
uvqRSQtg3gILW6AHgDs=
-----END SIGNATURE-----
-----END TEXT CERTIFICATE-----

Akenti Application: Monitoring

The **root policy** file is:

UserIdCertificateAuthority "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "-----BEGIN CERTIFICATE-----\
MIICdDCCAd2gAwIBAgIBATANBgkqhkiG9w0BAQQFADBeMQswCQYDVQ\ QGEwJVUzEuMCwGA1UEChMlTGF3cmVuY2UgQmVya2VsZXkgTnF0aWS\
sGA1UECxMESUNTRDEQMA4GA1UEAxMHSURDRy17DQTAeFw05NzA4MjkxNjMwNDJaFw05OTA4MjkxNj\
MwNDJaMF4xCzAJBgNVBAYTAlVTMS4wLAYDVQQKEyVMYXdyZW5jZSBCZXJrZWxleSBOYXRpb25hbC\
BMYWJvcmF0b3J5MQ0wCwYDVQQLEwRJQ1NEMRAwDgYDVQQDEwdJRENHLUNBMIGfMA0GCSqGSIb3DQ\
EBAQUAA4GNADCBiQKBgQDArly+tnX5eW7v4KT5CVf/IwR8rDkqniDUq34x/wqrKbM0AY+SV2hEHz\
+MCDgSlmPOXfwEplXW5IYYXqJ3+dK06et7mUodOhAB+0b6a8dVwul1+gRwEi80vft4+WvDUUHMZQ\
iq3UqFTsPN+09sW+2paqXNQZvBq2r+6/ovM4OqVwIDAQABo0IwQDAdBgNVHQ4EFgQUCQcdqlLvwV\
prM7kLlPL17fmW4PswHwYDVR0jBBgwFoAUCQcdqlLvwVprM7kLlPL17fmW4PswDQYJKoZIhvcNAQ\
EEBQADgYEAtcWt79TvzTl+zlkXBrn8lqJPLXfsmwn0eaUGZiBkxhm5FGMUs02sUjaAUKiC6seR9xN\
E2C6EEJ7OyZRP7aqtNbbqeZBnUtCJN/iyFk9vQMMtJtTPr6uBbExhUaGFuJLMhHfMG/1pfDTIHQZ\ 10Q0sF1ZmLyAdhiQBXekI5c5iheP4=\-----END

#UserIdCertificateAuthority "/C=US/O=Diesel Combustion Collaboratory/OU=SNL/CN=DieselCert.ca.sandia.gov" "-----BEGIN
CERTIFICATE-----\MIICiDCCAfGgAwIBAgIBATANBgkqhkiG9w0BAQQFADBoMQswCQYD\ VQQGEwJVUzEoMCYGA1UEChMfRGllc2VsIENvbWJ1c\
CxMDU05MMSEwHwYDVQQDExhEaWVzZWxrDZXJ0LmNhLnNhbnRpYS5nb3YwHhcNOTgwNDI3MTc1NTIw\
WhcNMDAwNDI2MTc1NTIwWjBoMQswCQYDVQQGEwJVUzEoMCYGA1UEChMfRGllc2VsIENvbWJ1c3Rp\
b24gQ29sbGFib3JhdG9yeTEMMAoGA1UECxMDU05MMSEwHwYDVQQDExhEaWVzZWxrDZXJ0LmNhLnNh\
bnRpYS5nb3YgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALzWQJ/+kXTzJMZoJMACjJI+nSEh\ u9P8qq8Q6NFgdPgriFVE6tggLcFWHzI6kgvv7i\
7DN93LWqlpCSchlu/sJWjwLtRSACr91C8LQKCGTWr9Ln58Ohh99wIBHeKYoSjcRWVi+pAgMBAAGj\
QjBAMB0GA1UdDgQWBBTHMjfik68SFzDCA6Ji6pU61+e5iTAfBgNVHSMEGDAWgBTHMjfik68SFzDC\
A6Ji6pU61+e5iTANBgkqhkiG9w0BAQQFAAOBgQCJpjUkl75PUrrn9h3lwt6MmmilelMQGts2X5q3d\ eSxBkiPPS9paMrN8UTY/mkVC6ZwQOlZ9oplBN+w\
4XyLOM6yUtClbZW3gzKvZtDKTjd+MPFARUaUanBqrnkJ3jCNA3yh0Acf2ow==\-----END CERTIFICATE-----"
CertificateDirectory public ldap idcg-ds.lbl.gov
#CertificateDirectory public ldap www-collab.ca.sandia.gov
#CertificateDirectory public web george.lbl.gov
#CertificateDirectory trusted file /home/u2/users/mudumbai/Newcerts
UseConditionCAandIssuer "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley National La
UseCondRequired http://www-itg.lbl.gov/~mrt/Certificates/

Pulling UseConditionCertificate http://www-itg.lbl.gov/~mrt/Certificates/
reqstr is: GET /~mrt/Certificates/ HTTP/1.0
Pulling UseConditionCertificate http://www-itg.lbl.gov/~mrt/Certificates/9ba89106.0
reqstr is: GET /~mrt/Certificates/9ba89106.0 HTTP/1.0

Akenti Application: Monitoring

```
Use Condition Certificate is:


-----BEGIN TEXT CERTIFICATE-----
-----BEGIN TEXT-----
use-condition
UID "rocky.lbl.gov#9ba89106#Wed Jun 10 14:00:13 PDT 1998"
issuerAndCA "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley National Laboratory/OU=
resource http://imglib.lbl.gov
scope sub-tree
attribute "( o : Lawrence Berkeley National Laboratory or o : Diesel Combustion Collaboratory )"
enable access read,execute
attributeIssuerAndCA o "Lawrence Berkeley National Laboratory" X509 "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA
Laboratory/OU=ICSD/CN=IDCG-CA"
attributeIssuerAndCA o "Diesel Combustion Collaboratory" X509 "/C=US/O=Diesel Combustion Collaboratory/OU=SNL/CN=DieselCert.ca.sandia.g
Collaboratory/OU=SNL/CN=DieselCert.ca.sandia.gov"
subjectCA "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA"
subjectCA "/C=US/O=Diesel Combustion Collaboratory/OU=SNL/CN=DieselCert.ca.sandia.gov"
-----END TEXT-----
-----BEGIN SIGNATURE-----
E3W+dElaMLI6Q7kfF3lpLR5GfPFmEI7Kd/aGaK+I8O/LBWBLxCOf+fN8Spb0756dnYZlfEsLhwzc
GEvGiCBMBoXYXL+f3hbnHActnDgtXWU3LaWpzu/mWXX4C2YkX5gcN6vjoKarkU5zfZFe+3lYE2vk
frfXBoIGtfcLNt7bnlo=
-----END SIGNATURE-----
-----END TEXT CERTIFICATE-----
```

Akenti Application: Monitoring

Notes

Unless otherwise noted, these paper are on the Web, and pointers may be found at http://www-itg.lbl.gov/~johnston/papers .

[1] "The NetLogger Methodology for High Performance Distributed Systems Performance Analysis,"
Brian Tierney, W. Johnston, J. Lee, G. Hoo, C. Brooks, D. Gunter. 7th IEEE Symposium on High Performance Distributed Computing, Chicago, Ill. July 29-31, 1998.

[2] "Authorization and Attribute Certificates for Widely Distributed Access Control,"
William Johnston, S. Mudumbai, and M. Thompson. IEEE 7th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises - WETICE'98, Stanford, CA. June, 1998.

[3] "Real-Time Generation and Cataloguing of Large Data-Objects in Widely Distributed Environments,"
W.Johnston, Jin G., C. Larsen, J. Lee, G. Hoo, M. Thompson, and B. Tierney (LBNL) and J. Terdiman (Kaiser Permanente Division of Research). Invited paper, International Journal of Digital Libraries - Special Issue on "Digital Libraries in Medicine". May, 1998.

[4] Akenti
PKI, Attribute, and Use-Condition certificate based access control with distributed management of multi-party policy.
See http://www-itg.lbl.gov/security/Akenti

[5] diffserv
"There is a clear need for relatively simple and coarse methods of providing differentiated classes of service for Internet traffic, to support various types of applications, and specific business requirements. The differentiated services approach to providing quality of service in networks employs a small, well- defined set of building blocks from which a variety of services may be built."
http://www.ietf.org/html.charters/diffserv-charter.html

[6] WALDO
"The Wide Area Large Data Object Architecture: We are exploring the use of highly distributed computing and storage architectures to provide all aspects of collecting, storing, analyzing, and accessing large data-objects. These data-objects can be anywhere from tens of MBytes to tens of GBytes in size. They are typically the result of a single operational cycle of an instrument, such as: single large images from electron microscopes, video images from cardio-angiography, sets of related images from MRI procedures and images and numerical from a particle accelerator experiment. The source of such data objects, e.g. centralized health care facilities or large scientific instruments is often remote from the users of the data and from available large-scale storage and computation systems."
"Our Large Data-object Architecture utilizes a high-speed wide-area ATM network between the object sources and a mutli-level distributed storage system (DPSS). As the data is being stored, a cataloguing system (ImgLib) automatically creates and stores condensed versions of the data, textual metadata and pointers to the original data. The catalogue system provides a Web based graphical

Akenti Application: Monitoring

interface to the data. The user is able the view the low-resolution data with a standard internet connection and Web browser, or if high-resolution is required can use a high-speed connection and special application programs to view the high-resolution original data."
See http://www-itg.lbl.gov/WALDO